Vereinbarung über die Auftragsverarbeitung (gemäß Art. 28 DSGVO)

zwischen

dem Empfänger des vorstehenden Angebotes

- nachstehend „Auftraggeber“ genannt -

und

Flowtify GmbH

Holzmarkt 59-65

50676 Köln

- nachstehend „Auftragnehmer“ genannt -

Inhaltsverzeichnis:

Präambel
Der Auftraggeber möchte den Auftragnehmer mit den in § 3 dieses Auftragsverarbeitungsvertrags genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen
(1) **Auftragsverarbeiter** ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
(2) **Personenbezogene Daten** sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
(3) **Verarbeitung** ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
(4) **Aufsichtsbehörde** ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde
(1) Zuständige Aufsichtsbehörde für den Auftraggeber ist der Landesbeauftragte für den Datenschutz des Bundeslandes des Auftraggebers.
(2) Zuständige Aufsichtsbehörde für den Auftragnehmer ist die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen.
(3) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Gegenstand des Auftrags
(1) Der Auftragnehmer erbringt für den Auftraggeber die in dem vorstehenden flowtify Vertrag („Hauptvertrag“) genannten Leistungen. Dabei verarbeitet der Auftragnehmer personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.
(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien den vorliegenden Vertrag. Die Regelungen des vorliegenden Vertrages gehen im Zweifel den Regelungen des Hauptvertrags vor.
(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.
(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, weist er den Auftraggeber darauf hin. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist ebenfalls in Anlage 1 dargestellt.

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 2 aufgeführten Maßnahmen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der betriebliche Ansprechpartner für den Datenschutz ist erreichbar unter privacy@flowtify.de.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer gewährleistet, dass alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- / Verschwiegenheitspflicht besteht auch nach Beendigung des Vertrages fort.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.
(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber kann sich von den technischen und organisatorischen Maßnahmen des Auftragnehmers überzeugen. Hierfür kann er nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.
(2) Der Auftragnehmer stellt dem Auftraggeber auf dessen schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.
(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 3 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Der Auftragnehmer informiert den Auftraggeber über eine Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Subunternehmern. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben. Der Auftragnehmer wählt die Subunternehmer sorgfältig nach deren Eignung, Zuverlässigkeit und Verarbeitungsstandort (Grundsätzlich im europäischen Wirtschaftsraum (EWR)) aus. Begründet der Auftragnehmer weitere Subunternehmerverhältnisse, obliegt es ihm, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den Subunternehmer zu übertragen. Sollten ausnahmsweise Drittlandtransfers außerhalb des EWR stattfinden, werden die Vorgaben des Art. 44 ff. DS-GVO eingehalten.
(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 bis 36 DS-GVO.
(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 Haftung gem. Art. 82 DS-GVO

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer grundsätzlich der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) 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.

§ 12 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Düsseldorf.

Anlage 1 zum AVV

Beschreibung der Daten/Datenkategorien, des Zwecks der Datenverarbeitung sowie der Betroffenen/Betroffenengruppen

Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenerhebung, -verarbeitung oder -nutzung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	**Zweck der Datenverarbeitung**	**Betroffene**
Benutzerdaten von Mitarbeitern • Vorname • Nachname • E-Mailadresse	• Verwaltung des Zugriffs (Login, Berechtigungen etc.)	• Mitarbeiter des Auftraggebers • Externe Personen, die der Auftraggeber benennt
Daten, die Benutzer während der Nutzung erfassen können: • Mitarbeiter- / Benutzerdaten • Unterschriften • Texteingaben • Fotos • Fotobeschreibungen • Zahlenabfragen • Ja / Nein Abfragen • Datum / Uhrzeit Abfragen • Single / Multiple Choice Abfragen • QR- oder Strichcode Abfragen • Ggf. hochgeladene Dokumente mit personenbezogenen Inhalten	Nutzung der flowtify Applikation zur papierlosen Eigendokumentation, Eigenkontrolle sowie anderen Dokumentationszwecken einmaliger oder wiederkehrender Tätigkeiten, um Betriebsabläufe zu strukturieren, organisieren oder optimieren.	• Auftraggeber • Mitarbeiter des Auftraggebers • Externe Personen, die der Auftraggeber benennt • Externe Personen, deren Daten dem Auftragnehmer vom Auftraggeber, einem Mitarbeiter des Auftraggebers oder einer externen Person, die der Auftraggeber benannt hat, übermittelt worden sind
Stammdaten des Auftraggebers • Firmenname • Ansprechpartner • Anschrift • E-Mailadresse • Telefonnummer	Korrespondenz mit dem Auftraggeber	• Ansprechpartner • Beauftragende Person des Auftraggebers

Anlage 2 zum AVV

Technische und organisatorische Maßnahmen des Auftragnehmers i. S. d. Art. 32 DS-GVO

In den Büroräumlichkeiten der Flowtify GmbH werden keine Server betrieben.

Vertraulichkeit

Zutrittskontrolle

- Das Firmengebäude ist vollständig umfriedet
- Das Firmengebäude besitzt ein manuelles Schließsystem
- Die Zugangstür besitzt einen Knauf an der Außenseite
- Jeder Mitarbeiter erhält einen Schlüssel für das Firmengebäude
- Die Vergabe der Schlüssel wird dokumentiert und regelmäßig überprüft
- Besucher werden immer durch mindestens einen Mitarbeiter der Flowtify GmbH begleitet
- Die Dienstleister werden sorgfältig ausgewählt

Zugangskontrolle

- Die Vergabe und Verwaltung von Benutzerrechten für einzelne Systeme erfolgt ausschließlich durch Systemadministratoren.
- Alle Arbeitsgeräte, auf denen personenbezogene Daten verarbeitet werden, sind für den jeweiligen Mitarbeiter personalisiert, mit einem Passwort geschützt und verwenden das aktuelle Betriebssystem
- Mitarbeiter sind angewiesen Ihren Arbeitsplatz bei Verlassen zu sperren
- Mitarbeiter sind angewiesen Ihren Arbeitsplatz sauber zu halten und Unterlagen mit personenbezogenen Daten unzugänglich für Dritte aufzubewahren. (Clean desk policy)
- Für die Verwendung eines sicheren Passworts gelten folgende Regelungen: - mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen, und eine Zahl enthalten, sowie mindestens 12 Zeichen lang sein müssen.
- In allen Systemen sind, soweit vorhanden, die Sicherheitsmaßnahme der „2-Faktor-Authentifizierung“ für jeden Benutzer standardmäßig aktiviert.

Zugriffskontrolle

- Definierte Benutzergruppen
- Jedem Benutzer ist ein eigener Login zugeordnet
- Trennung von Systemdateien unterschiedlicher Anwendungen
- Trennung von Benutzerdateien verschiedener Benutzer
- Benutzung eines Akten Schredders
- Minimale Anzahl an Administratoren

Trennungskontrolle

- Trennung von Entwicklungs-, Test- und Produktivumgebung
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Mandantenfähigkeit relevanter Anwendungen
- Steuerung über Berechtigungskonzept

Pseudonymisierung

- Pseudonymisierung wird nach Möglichkeit angewendet
- Trennung der Zuordnungsdaten
- Personenbezogene Daten werden im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst anonymisiert / pseudonymisiert

Integrität

Weitergabekontrolle
- Gesicherter Datentransport (SSL)
- Datenträgerverschlüsselung
- Nach Möglichkeit automatisierte E-Mail Verschlüsselung

Eingangskontrolle
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten durch individuelle Benutzernamen
- Klare Zuständigkeiten für Löschungen

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle
- Regelmäßige Updates der eingesetzten Software
- Backup & Recovery Konzept
- Regelmäßige Tests zur Datenwiederherstellung

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Maßnahmen
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Dokumentation einer Übersicht über die Verarbeitungstätigkeiten
- Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird jährlich durchgeführt
- Interner Datenschutzbeauftragter: Parshin Mortazi, Flowtify GmbH, privacy@flowtify.de
- Regelmäßige Sensibilisierung der Mitarbeiter auf Datengeheimnis

Incident-Response-Management
- Meldeprozess für Datenschutzverletzungen gegenüber Datenschutzbehörden vorhanden
- Meldeprozess für Datenschutzverletzungen gegenüber Betroffenen vorhanden

Datenschutzfreundliche Voreinstellungen
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

Auftragskontrolle
- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere in Bezug auf Datenschutz und
  -sicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Verpflichtung zur Bestellung eines Datenschutzbeauftragen durch den Auftragnehmer bei vorliegender Bestellpflicht
- Regelung zum Einsatz weiterer Subunternehmer
- Regelmäßige Überprüfung des Auftragnehmers und seines Schutzniveaus

Anlage 3 zum AVV

Beauftragte Subunternehmer:

Derzeit sind nachfolgende Subunternehmer vom Auftragnehmer beauftragt:

Microsoft Ireland Operations, Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521

- Hosting
- Standort Hosting: Frankfurt am Main (Deutschland)
- https://www.microsoft.com/de-de/cloud/compliance
- https://www.microsoft.com/en-us/licensing/product-licensing/products

Salesforce.com Germany GmbH, Erika-Mann-Str. 63, 80636 München, Deutschland

- Kundenmanagement & Kundenservice
- Standort Hosting: Frankfurt am Main (Deutschland)
- https://status.salesforce.com/search/flowtify
- https://compliance.salesforce.com/en
- https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf

Die technischen organisatorischen Maßnahmen der Subunternehmer sind auf den folgenden Seiten aufgeführt.

Technische und organisatorische Maßnahmen Microsoft Ireland Operations, Ltd.

Organisation der IT-Sicherheit

Verantwortung für die Sicherheit

- Microsoft hat einen oder mehrere Sicherheitsbeauftragte ernannt, die für die Koordination und Überwachung der Sicherheitsregeln und -verfahren verantwortlich sind.

Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit

- Microsoft-Mitarbeiter, die Zugang zu Kundendaten haben, sind zur Vertraulichkeit verpflichtet.

Risikomanagementprogramm

- Microsoft führte eine Risikobewertung durch, bevor die Kundendaten verarbeitet oder die Onlinedienste-Leistungen gestartet wurden.
- Microsoft archiviert Sicherheitsunterlagen im Rahmen der Aufbewahrungspflichten, nachdem sie nicht mehr in Kraft sind.

Asset-Management

Anlagenbestand

- Microsoft führt einen Bestand aller Medien, auf denen Kundendaten gespeichert sind. Der Zugriff auf die Bestände solcher Medien ist auf Microsoft-Mitarbeiter beschränkt, die schriftlich dazu berechtigt sind.

Asset-Handling

- Microsoft klassifiziert Kundendaten, um die Identifizierung zu erleichtern und eine angemessene Beschränkung des Zugriffs auf Kundendaten zu ermöglichen.
- Microsoft legt Einschränkungen für das Drucken von Kundendaten fest und verfügt über Verfahren für die Entsorgung gedruckter Materialien, die Kundendaten enthalten.
- Mitarbeiter von Microsoft müssen eine Genehmigung von Microsoft einholen, bevor sie

Kundendaten auf tragbaren Geräten speichern, remote auf Kundendaten zugreifen oder Kundendaten außerhalb der Einrichtungen von Microsoft verarbeiten.

Personalsicherheit

Sicherheitsschulungen

- Microsoft informiert seine Mitarbeiter über relevante Sicherheitsverfahren und ihre jeweiligen Rollen. Microsoft informiert seine Mitarbeiter auch über mögliche Folgen einer Verletzung der Sicherheitsregeln und -verfahren. Microsoft verwendet in der Schulung nur anonyme Daten.

Physische und umgebungsbezogene Sicherheit

Physischer Zugang zu Einrichtungen

- Microsoft beschränkt den Zugang zu Einrichtungen, in denen sich Kundendaten verarbeitende Informationssysteme befinden, auf identifizierte, autorisierte Personen.

Physischer Zugriff auf Komponenten

- Microsoft führt Aufzeichnungen über die ein- und ausgehenden Medien, die Kundendaten enthalten, einschließlich der Art der Medien, des zugelassenen Absenders/der zugelassenen Empfänger, Datum und Uhrzeit, der Anzahl von Medien und der darin enthaltenen Arten von Kundendaten.

Schutz vor Unterbrechungen

- Microsoft nutzt eine Vielzahl von branchenüblichen Systemen, um den Verlust von Daten durch Stromausfall oder Leitungsstörungen zu verhindern.

Entsorgung von Komponenten

- Microsoft verwendet branchenübliche Prozesse, um Kundendaten zu löschen, wenn sie nicht mehr benötigt werden.

Kommunikations- und Betriebsmanagement

Betriebsrichtlinie

- Microsoft führt Sicherheitsunterlagen, in denen die Sicherheitsmaßnahmen sowie die entsprechenden Verfahren und Verantwortlichkeiten der Mitarbeiter beschrieben sind, die Zugang zu Kundendaten haben.

Datenwiederherstellungsverfahren

- Microsoft erstellt kontinuierlich, mindestens jedoch einmal pro Woche (es sei denn, es wurden im betreffenden Zeitraum keine Kundendaten aktualisiert) mehrere Kopien von Kundendaten, aus denen Kundendaten wiederhergestellt werden können.
- Microsoft bewahrt Kopien von Kundendaten und Datenwiederherstellungsverfahren an einem anderen Ort als dem auf, an dem sich die primären Computergeräte befinden, von denen die Kundendaten verarbeitet werden.
- Microsoft verfügt über bestimmte Verfahren, die den Zugriff auf Kopien von Kundendaten regeln.
- Microsoft prüft die Datenwiederherstellungsverfahren mindestens einmal alle sechs Monate. Ausgenommen hiervon sind Verfahren für Azure Government Services, die alle zwölf Monate geprüft werden.
- Microsoft protokolliert Datenwiederherstellungsmaßnahmen. Dabei werden Informationen zur verantwortlichen Person, die Beschreibung der wiederhergestellten Daten sowie gegebenenfalls Angaben zu den Daten, die bei der Datenwiederherstellung manuell eingegeben werden mussten, aufgezeichnet.

Malware

- Microsoft nimmt Anti-Schadsoftware-Kontrollen vor, um zu verhindern, dass bösartige Software unbefugten Zugriff auf Kundendaten erhält, einschließlich bösartiger Software aus öffentlichen Netzwerken.

Daten außerhalb von Landesgrenzen

- Microsoft verschlüsselt Kundendaten, die über öffentliche Netzwerke übermittelt werden, oder ermöglicht dem Kunden eine solche Verschlüsselung.
- Microsoft schränkt den Zugriff auf Kundendaten in Medien ein, die die Einrichtungen von Microsoft verlassen.

Ereignisprotokollierung

- Microsoft protokolliert den Zugriff und die Nutzung von Informationssystemen, die Kundendaten enthalten, indem die Zugangs-ID, die Uhrzeit, die erteilte oder verweigerte Berechtigung und die entsprechende Aktivität registriert werden, oder ermöglicht dem Kunden eine Protokollierung.

Zugriffskontrolle

Zugriffsrichtlinie

- Microsoft führt eine Aufzeichnung der Sicherheitsberechtigungen von Einzelpersonen, die Zugang zu Kundendaten haben.

Zugriffsberechtigung

- Microsoft führt und aktualisiert Aufzeichnungen zu den Mitarbeitern, die zum Zugriff auf Microsoft-Systeme autorisiert sind, die Kundendaten enthalten.
- Microsoft deaktiviert Anmeldedaten, die über einen bestimmten Zeitraum, der sechs Monate nicht überschreiten darf, nicht verwendet wurden.
- Microsoft benennt diejenigen Mitarbeiter, die berechtigt sind, den autorisierten Zugriff auf Daten und Ressourcen zu gewähren, zu ändern oder zu widerrufen.
- Wenn mehrere Personen Zugriff auf die Systeme haben, in denen Kundendaten enthalten sind, stellt Microsoft sicher, dass diese Personen über separate Kennungen/Anmeldedaten verfügen.

Geringste Rechte

- Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur gestattet, wenn dies erforderlich ist.
- Microsoft schränkt den Zugriff auf Kundendaten auf solche Personen ein, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen.

Integrität und Vertraulichkeit

- Microsoft weist Mitarbeiter an, Administrationssitzungen zu deaktivieren, wenn sie Einrichtungen, die sich unter der Kontrolle von Microsoft befinden, verlassen oder wenn Computer anderweitig unbeaufsichtigt sind.
- Microsoft speichert Kennwörter so, dass sie während des Gültigkeitszeitraums nicht erkennbar sind.

Authentifizierung

- Microsoft verwendet Verfahren nach Branchenstandard, um Benutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen.
- Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass die Kennwörter regelmäßig erneuert werden müssen.
- Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass das Kennwort mindestens acht Zeichen umfassen muss.
- Microsoft stellt sicher, dass deaktivierte oder abgelaufene Kennungen an keine andere Person vergeben werden.
- Microsoft überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf Informationssysteme zu verschaffen, oder ermöglicht dem Kunden eine solche Überwachung.
- Microsoft unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die manipuliert oder versehentlich offengelegt wurden.
- Microsoft verwendet Verfahren nach Branchenstandard zum Schutz von Kennwörtern, einschließlich Verfahren, die die Vertraulichkeit und Integrität von Kennwörtern während der Zuweisung und Verteilung sowie während der Speicherung wahren sollen.

Netzwerkdesign

- Microsoft führt Kontrollen durch, um zu verhindern, dass Personen Zugriffsrechte erhalten, die ihnen nicht zugewiesen wurden, um Zugang zu Kundendaten zu erhalten, auf die sie nicht zugreifen dürfen.

Handhabung eines Informationssicherheitsvorfalls

Vorfallreaktionsablauf

- Microsoft führt Unterlagen über Sicherheitsverletzungen unter Angabe einer Beschreibung der Verletzung, des Zeitraums, der Konsequenzen der Verletzung, des Namens der Person, die den

Zwischenfall gemeldet hat, und der Person, der der Zwischenfall gemeldet wurde, sowie des Verfahrens für die Wiederherstellung von Daten.

- Für jede Sicherheitsverletzung, bei der es sich um einen Sicherheitsvorfall handelt, erfolgt (wie im Abschnitt „Meldung von Sicherheitsvorfällen“ weiter oben beschrieben) unverzüglich und auf jeden Fall innerhalb von 72 Stunden eine Benachrichtigung seitens Microsoft.
- Microsoft untersucht Offenlegungen von Kundendaten, einschließlich der Fragen, welche Daten offengelegt wurden, gegenüber wem und zu welchem Zeitpunkt, oder versetzt den Kunden dazu in die Lage.

Dienstüberwachung

- Das Microsoft-Sicherheitspersonal überprüft die Protokolle mindestens alle sechs Monate, um gegebenenfalls Abhilfemaßnahmen vorzuschlagen.

Geschäftsfortführungsmanagement

- Microsoft unterhält Notfall- und Alternativpläne für die Einrichtungen, in denen sich Microsoft Informationssysteme befinden, die Kundendaten verarbeiten.
- Der redundante Speicher von Microsoft sowie die Verfahren von Microsoft zur Wiederherstellung von Daten sind so konzipiert, dass versucht wird, Kundendaten in ihrem ursprünglichen oder ihrem zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren.

Technische und organisatorische Maßnahmen Salesforce.com Germany GmbH

Architektur und Datentrennung

Die Abgedeckten Dienste werden in einer mandantenfähigen Architektur betrieben, die darauf ausgelegt ist, den Zugriff auf Kundendaten zu trennen und zu beschränken Zugriff auf Kundendaten auf der Grundlage von Geschäftsanforderungen. Die Architektur bietet eine effektive logische Datentrennung für verschiedene Kunden über kundenspezifische "Organisations-IDs" und ermöglicht die Verwendung von und rollenbasierte Zugriffsrechte für Benutzer. Eine zusätzliche Datentrennung wird gewährleistet durch die Bereitstellung separater Umgebungen für verschiedene Funktionen, insbesondere für Test und Produktion.

Steuerung der Verarbeitung

Salesforce hat Verfahren implementiert, die sicherstellen sollen, dass die Kundendaten nur gemäß den der gesamten Kette von Verarbeitungstätigkeiten durch Salesforce und seine Unterauftragsverarbeiter nur gemäß den Anweisungen des Kunden verarbeitet werden. Insbesondere haben Salesforce und seine verbundenen Unternehmen mit ihren Unterauftragsverarbeitern schriftliche Vereinbarungen getroffen, die Verpflichtungen zum Schutz der Privatsphäre, des Datenschutzes und der Datensicherheit enthalten und ein Schutzniveau bieten, das für ihre Verarbeitungstätigkeiten angemessen ist. Die Einhaltung dieser Verpflichtungen sowie die technischen und organisatorischen Datensicherheitsmaßnahmen, die von Salesforce und seinen Unterverarbeitern sind Gegenstand regelmäßiger Audits.

Funktionalitäten von Drittanbietern

Bestimmte Funktionen der Abgedeckten Dienste nutzen Funktionen, die von Dritten bereitgestellt werden. Die Account Intelligence-Funktion in Sales Cloud - Account News, Lightning News, Account Logos und Account Autofill funktionieren durch das Senden von Standardfeldern aus dem Account-Objekt des Kunden an die Einstein-Plattform von Salesforce gesendet werden, die derzeit von AWS gehostet wird, wo diese Daten mit Inhalten, wie z. B. Nachrichtenartikeln, abgeglichen werden, die über Sales Cloud zur Verfügung gestellt werden. Kunden können die Account Intelligence-Funktionen deaktivieren.

Wenn Kunden Messaging verwenden, um mobile Nachrichten, wie z. B. SMS-Nachrichten, zu senden oder zu empfangen, werden die Inhalt dieser Nachrichten und damit verbundene Informationen über diese Nachrichten von

(a) Aggregatoren - Unternehmen, die als Vermittler bei der Übertragung von Mobilfunknachrichten oder der Bereitstellung von Mobilfunknummern fungieren, und

(b) Carrier - Unternehmen, die drahtlose Nachrichtendienste für Teilnehmer über drahtlose oder drahtgebundene Telekommunikationsnetzwerke anbieten. Solche Aggregatoren und Carrier greifen auf Nachrichteninhalte und zugehörige Informationen zu, speichern diese und übertragen sie und zugehörige Informationen, um diese Funktionen bereitzustellen. Bei Over-the-Top-Messaging-Diensten, wie z. B. Facebook Messenger und WhatsApp, werden die Inhalte der über einen solchen Dienst gesendeten oder empfangenen Nachrichten und damit zusammenhängende Informationen über solche Nachrichten werden von Einrichtungen empfangen, die solche Over-the-Top-Messaging-Dienste ermöglichen.

Audits und Zertifizierungen

Die folgenden sicherheits- und datenschutzbezogenen Prüfungen und Zertifizierungen gelten für einen oder mehrere der Abgedeckten Dienste finden Sie hier.

Darüber hinaus werden die Abgedeckten Dienste mindestens einmal jährlich Sicherheitsbewertungen durch interne Mitarbeiter und Dritte unterzogen, die Bewertungen der Schwachstellen der Infrastruktur und der Anwendungssicherheit umfassen.

Salesforce nutzt die von Amazon Web Services, Inc. bereitgestellte Infrastruktur. ("AWS"), um Kundendaten zu hosten oder zu verarbeiten, die an bestimmte Abgedeckte Services und Funktionen übermittelt werden. Informationen über sicherheits- und datenschutzbezogene Audits und Zertifizierungen, die AWS erhalten hat, einschließlich ISO 27001-Zertifizierung und SOC- Berichte, sind auf der AWS Security-Website und der AWS Compliance-Website verfügbar.

Salesforce verwendet die von Heroku bereitgestellte Infrastruktur, um Kundendaten zu hosten oder zu verarbeiten, die an bestimmte Abgedeckte Services und Funktionen übermittelt werden. Informationen über sicherheits- und datenschutzbezogene Prüfungen und Zertifizierungen, die Heroku erhalten hat, einschließlich der ISO 27001-Zertifizierung und SOC-Berichte, sind in der Dokumentation zu Sicherheit, Datenschutz und Architektur von Heroku verfügbar.
Sicherheitskontrollen
Die Abgedeckten Dienste enthalten eine Vielzahl von konfigurierbaren Sicherheitskontrollen, die es den Kunden ermöglichen, die Sicherheit der Abgedeckten Dienste für ihre eigene Nutzung anzupassen. Weitere Informationen zu solchen Kontrollen finden Sie in dem Salesforce Security Guide. Informationen zur Multi-Faktor-Authentifizierung und Single Sign-On für den Zugriff auf
die Abgedeckten Services sind in den jeweiligen Hinweisen und Lizenzinformationen (NLI) aufgeführt.

Bestimmte Abgedeckte Services und Funktionen nutzen AWS, um Kundendaten zu hosten oder zu verarbeiten; weitere Informationen zur Sicherheit, die von AWS bereitgestellt wird, sind auf der AWS-Sicherheitswebsite verfügbar, einschließlich der Übersicht von AWS über Sicherheits
Prozesse.
Bestimmte Abgedeckte Services und Funktionen nutzen die Heroku-Plattform, um Kundendaten zu hosten oder zu verarbeiten; weitere Informationen über die von Heroku bereitgestellte Sicherheit finden Sie in der Dokumentation zu Sicherheit, Datenschutz und Architektur von Heroku.

Sicherheitsrichtlinien und -prozeduren

Die Abgedeckten Dienste werden in Übereinstimmung mit den folgenden Richtlinien und Verfahren betrieben, um die Sicherheit zu erhöhen:

- Kundenpasswörter werden mit einem one-way salted Hash gespeichert.
- Es werden Benutzerzugriffsprotokolleinträge geführt, die Datum, Uhrzeit, Benutzer-ID, ausgeführte URL oder Entity-ID, durchgeführte Operation (erstellt, aktualisiert, gelöscht) und Quell-IP-Adresse. Beachten Sie, dass Quell-IP-Adresse möglicherweise nicht verfügbar ist, wenn NAT (Network Address Translation) oder PAT (Port Address Translation) vom Kunden oder seinem ISP verwendet wird.
- Wenn der Verdacht eines unangemessenen Zugriffs besteht, kann Salesforce den Kunden Protokolleinträge zur Verwendung in der forensischen Analyse zur Verfügung stellen, wenn diese verfügbar sind. Dieser Service wird den Kunden auf einer Zeit- und Materialbasis zur Verfügung gestellt.

- Die Protokolle des physischen Zugriffs auf das Rechenzentrum, der Systeminfrastruktur und der Anwendungen werden mindestens 90 Tage lang aufbewahrt. Die Protokolle werden in einem sicheren Bereich aufbewahrt, um Manipulationen zu verhindern.
- Passwörter werden nicht protokolliert.
- Bestimmte administrative Änderungen an den Abgedeckten Diensten (z. B. Passwortänderungen und Hinzufügen von benutzerdefinierte Felder) werden in einem als "Setup Audit Trail" bezeichneten Bereich nachverfolgt und sind zur Ansicht verfügbar durch den Systemadministrator eines Kunden. Kunden können diese Daten herunterladen und lokal speichern.
- Das Salesforce-Personal legt kein definiertes Passwort für einen Benutzer fest. Passwörter werden auf einen Zufallswert zurückgesetzt (der bei der ersten Verwendung geändert werden muss) und automatisch per E-Mail an den anfragenden Benutzer gesendet wird.

Intrusion Detection

Salesforce oder ein autorisierter Dritter überwacht die Abgedeckten Services auf unbefugtes Eindringen mit Hilfe von netzwerkbasierten und/oder hostbasierten Mechanismen zur Erkennung von Eindringlingen. Salesforce kann die von den Webbrowsern der Benutzer gesammelten Daten zu Sicherheitszwecken analysieren, einschließlich der Erkennung von kompromittierten Browsern, um betrügerische Authentifizierungen zu verhindern und um sicherzustellen, dass die Abgedeckten Services ordnungsgemäß funktionieren.

Sicherheitsprotokolle

Alle Systeme, die bei der Erbringung der Abgedeckten Dienste verwendet werden, einschließlich Firewalls, Router, Netzwerk-Switches und Betriebssysteme, protokollieren Informationen an ihre jeweilige Systemprotokollierungseinrichtung oder einen zentralen Syslog-Server (für Netzwerksysteme), um Sicherheitsüberprüfungen und -analysen zu ermöglichen.

Incident-Management

Salesforce unterhält Richtlinien und Verfahren für das Management von Sicherheitsvorfällen. Salesforce benachrichtigt betroffene Kunden unverzüglich über jede unbefugte Offenlegung ihrer jeweiligen Kundendaten durch Salesforce oder seine Vertreter, von der Salesforce Kenntnis erlangt, soweit dies gesetzlich zulässig ist.

Salesforce veröffentlicht Informationen zum Systemstatus auf der Salesforce Trust-Website. Salesforce benachrichtigt Kunden in der Regel per E-Mail über bedeutende Systemvorfälle und kann bei Vorfällen, die länger als eine Stunde dauern, die betroffenen Kunden zu einer Telefonkonferenz über den Vorfall und die Reaktion von Salesforce einladen.
Benutzerauthentifizierung

Der Zugriff auf Abgedeckte Services, mit Ausnahme von Experience Cloud (ehemals Community Cloud)-Gastbenutzern, erfordert eine Authentifizierung über einen der unterstützten Mechanismen, wie im Salesforce Security Guide beschrieben, einschließlich Benutzer-ID/Passwort, SAML-basierter Verbund, OpenID Connect, OAuth, Social Login oder delegierte Authentifizierung, wie vom Kunden bestimmt und kontrolliert. Nach erfolgreicher Authentifizierung wird eine zufällige Sitzungs-ID generiert und im Browser des Benutzers gespeichert, um den Sitzungsstatus zu erhalten und zu verfolgen.

Physische Sicherheit

Die Produktionsrechenzentren, die für die Erbringung der abgedeckten Dienstleistungen verwendet werden, verfügen über Zugangskontrollsysteme, die nur autorisiertem Personal den Zugang zu sicheren Bereichen ermöglichen. Diese Einrichtungen sind so konzipiert, dass sie widrigen Witterungsbedingungen und anderen einigermaßen vorhersehbaren natürlichen Bedingungen standhalten, verwenden redundante elektrische und Telekommunikationssysteme, setzen Umweltsysteme ein, die Temperatur, Luftfeuchtigkeit und andere Umgebungsbedingungen überwachen, und enthalten strategisch platzierte Wärme-, Rauch- und Branderkennungs- und Unterdrückungssysteme. Die Einrichtungen sind rund um die Uhr durch Wachpersonal, Überwachungskameras im Innen- und Außenbereich, eine Zwei-Faktor-Zugangskontrolle und

begleiteten Zugang gesichert. Im Falle eines Stromausfalls werden unterbrechungsfreie Stromversorgungen und kontinuierliche Stromversorgungslösungen eingesetzt, um die Stromversorgung zu gewährleisten, während die Systeme auf vor Ort vorhandene Notstromgeneratoren übertragen werden.

Ausfallsicherheit und Backup

Alle Netzwerkkomponenten, Netzwerkbeschleuniger, Load Balancer, Webserver und Anwendungsserver sind in einer redundanten Konfiguration konfiguriert. Alle Kundendaten, die an die Abgedeckten Dienste übermittelt werden, werden auf einem primären Datenbankserver mit mehreren aktiven Clustern für eine höhere Verfügbarkeit gespeichert. Alle Kundendaten, die an die Abgedeckten Dienste übermittelt werden, werden auf hochredundantem Plattenspeicher der Carrier-Klasse und mehreren Datenpfaden gespeichert, um Zuverlässigkeit und Leistung zu gewährleisten. Alle an die Abgedeckten Dienste übermittelten Kundendaten, bis zur letzten bestätigten Transaktion, wird automatisch und nahezu in Echtzeit zum sekundären Standort repliziert und in lokalisierten Datenspeichern gesichert. Backups werden auf Integrität geprüft und in denselben Rechenzentren wie ihre Instanz gespeichert.

Wiederherstellung im Katastrophenfall

Die Produktionsrechenzentren sind so konzipiert, dass sie das Risiko von Single Points of Failure mindern und eine belastbare Umgebung zur Unterstützung der Servicekontinuität und -leistung bereitstellen. Die abgedeckten Services nutzen sekundäre Einrichtungen, die sich geografisch von den primären Rechenzentren unterscheiden, zusammen mit der erforderlichen Hardware, Software und Internetkonnektivität für den Fall, dass die Salesforce-Produktionseinrichtungen in den primären Rechenzentren nicht mehr verfügbar sind.

Salesforce verfügt über Notfallwiederherstellungspläne und testet diese mindestens einmal pro Jahr. Der Umfang der Disaster-Recovery-Übung besteht darin, die Fähigkeit zum Failover einer Produktionsinstanz vom primären Rechenzentrum zum sekundären Rechenzentrum unter Verwendung der entwickelten Betriebs- und Disaster-Recovery-Verfahren und -Dokumentation zu validieren.

Die Notfallwiederherstellungspläne für die Abgedeckten Services haben derzeit die folgenden Zielvorgaben für die Wiederherstellung: (a) Wiederherstellung des Abgedeckten Service (Ziel für die Wiederherstellungszeit) innerhalb von 12 Stunden nach der Erklärung einer Katastrophe durch Salesforce; und (b) maximaler Verlust von Kundendaten (Ziel für den Wiederherstellungspunkt) von 4 Stunden. Diese Ziele schließen jedoch eine Katastrophe oder mehrere Katastrophen aus, die die Kompromittierung beider Rechenzentren zur gleichen Zeit verursachen, und schließen Entwicklungs- und Testbettumgebungen, wie den Sandbox-Service, aus.

Viren

Die Abgedeckten Dienste scannen nicht nach Viren, die in Anhängen oder anderen Kundendaten enthalten sein könnten, die von einem Kunden in die Abgedeckten Dienste hochgeladen werden. Hochgeladene Anhänge werden jedoch nicht in den Abgedeckten Diensten ausgeführt und können daher die Abgedeckten Dienste nicht dadurch beschädigen oder gefährden, dass sie einen Virus enthalten.

Datenverschlüsselung

Die Abgedeckten Dienste verwenden branchenübliche Verschlüsselungsprodukte, um Kundendaten und die Kommunikation während der Übertragungen zwischen dem Netzwerk des Kunden und den Abgedeckten Diensten zu schützen, u. a. durch Transport Layer Encryption (TLS) unter Verwendung von mindestens 2048-Bit-RSA-Serverzertifikaten und symmetrischen 128-Bit- Verschlüsselungsschlüsseln. Darüber hinaus werden alle Daten, einschließlich der Kundendaten, zu Replikationszwecken über verschlüsselte Verbindungen unter Verwendung von AES-256- Verschlüsselung zwischen Rechenzentren übertragen.

Rückgabe von Kundendaten

Innerhalb von 30 Tagen nach Vertragsbeendigung können Kunden die Rückgabe ihrer jeweiligen Kundendaten verlangen, die sie an die Abgedeckten Dienste übermittelt haben (sofern diese Daten nicht vom Kunden gelöscht wurden,

oder wenn Kunde (das verwaltete Paket, in dem die Kundendaten gespeichert waren, nicht bereits entfernt hat). Salesforce stellt solche Kundendaten über herunterladbare Dateien im Format "comma separated value" (.csv) und Anhänge in ihrem nativen Format zur Verfügung. Die vorgenannte Rückgabe von Kundendaten für verwaltete Pakete ist möglicherweise nicht verfügbar, wenn die Pakete vor der Vertragskündigung entfernt wurden.

Löschung von Kundendaten

Sofern nachstehend nichts anderes angegeben ist, werden Kundendaten, die an die Abgedeckten Services übermittelt wurden, nach Beendigung aller Abonnements, die mit einer Umgebung verbunden sind, innerhalb der Abgedeckten Services für 120 Tage in einem inaktiven Status aufbewahrt; danach werden sie innerhalb von 90 Tagen sicher überschrieben oder aus der Produktion und innerhalb von 180 Tagen aus den Sicherungen gelöscht. Physische Medien, auf denen Kundendaten während der Vertragslaufzeit gespeichert sind, werden nicht aus den Rechenzentren entfernt, die Salesforce zum Hosten von Kundendaten verwendet, es sei denn, die Medien sind am Ende ihrer Nutzungsdauer oder werden deprovisioniert; in diesem Fall werden die Medien vor der Entfernung zunächst bereinigt. Dieser Prozess unterliegt den geltenden gesetzlichen Anforderungen.

Ohne die Möglichkeit der Kunden einzuschränken, die Rückgabe ihrer an die Abgedeckten Services übermittelten Kundendaten zu verlangen, behält sich Salesforce das Recht vor, die Anzahl der Tage, die es diese Daten nach Vertragsbeendigung aufbewahrt, zu reduzieren. Salesforce wird diese Salesforce-Dokumentation zu Sicherheit, Datenschutz und Architektur im Falle einer solchen Änderung aktualisieren.

Tag 0, Abonnement wird beendet	Tag 0 - 30	Tag 30 - 120	Tag 121 - 211	Tag 121 - 301
	Daten zur Rücksendung an den Kunden verfügbar	Daten inaktiv und nicht mehr verfügbar	Daten aus der Produktion gelöscht oder überschrieben	Daten aus Sicherungen gelöscht oder überschrieben

Die vorgenannte Löschung von Kundendaten für verwaltete Pakete ist möglicherweise nicht verfügbar, wenn die Pakete vor der Vertragskündigung entfernt wurden.

Sensible Daten

Wichtig: Kunden müssen entweder "Plattform Encryption" für unterstützte Feldtypen und Dateianhänge oder die Funktion "Classic Encryption" für benutzerdefinierte Felder verwenden und den Lebenszyklus ihrer Verschlüsselungsschlüssel verwalten, wenn sie Daten von Zahlungskarteninhabern und Authentifizierungsdaten, Kredit- oder Debitkartennummern oder jegliche Sicherheitscodes oder Passwörter an die Abgedeckten Dienste übermitteln. Kunden dürfen solche Daten nicht anderweitig an die Abgedeckten Dienste übermitteln. Für andere Kategorien von sensiblen Daten sollten Kunden auch die Verwendung von "Plattform Encryption" oder "Classic Encryption" in Betracht ziehen.

Für Intelligent Form Reader gilt, dass der Kunde, wenn er einen Teil dieses Abgedeckten Dienstes in Verbindung mit einem Entscheidungsprozess mit rechtlichen oder ähnlich bedeutsamen Auswirkungen nutzen möchte, sicherstellen muss, dass die endgültige Entscheidung von einem Menschen getroffen wird.

Zur Klarstellung: Die vorstehenden Beschränkungen gelten nicht für Finanzdaten, die Salesforce zum Zwecke der Überprüfung der finanziellen Qualifikationen seiner Kunden und der Einziehung von Zahlungen zur Verfügung gestellt werden; die Verarbeitung dieser Daten unterliegt den Datenschutzbestimmungen der Salesforce-Website.

Analytik

Salesforce kann die Nutzung der Abgedeckten Services zu Sicherheitszwecken und zur Unterstützung von Salesforce bei der Verbesserung sowohl der Abgedeckten Services als auch der Benutzererfahrung bei der Nutzung der Abgedeckten Services verfolgen und analysieren. Zum Beispiel können wir diese Informationen verwenden, um Trends zu verstehen und zu analysieren oder zu verfolgen, welche unserer Funktionen am häufigsten verwendet werden, um die Produktfunktionalität zu verbessern.

Salesforce kann anonyme Nutzungsdaten an die Serviceanbieter von Salesforce weitergeben, um Salesforce bei der Nachverfolgung, Analyse und Verbesserung zu unterstützen. Darüber hinaus kann Salesforce solche anonymen Nutzungsdaten auf einer aggregierten Basis im Rahmen des normalen Geschäftsbetriebs weitergeben; so können wir beispielsweise Informationen öffentlich zugänglich machen, um Trends über die allgemeine Nutzung unserer Dienste aufzuzeigen.

Zusammenspiel mit anderen Diensten

Die Abgedeckten Services können mit anderen von Salesforce oder Dritten bereitgestellten Services interagieren oder integriert werden. Wenn Systeme von Drittanbietern eine Verbindung zu den Abgedeckten Services herstellen, stellen diese externen Systeme den Abgedeckten Services Metadaten zur Verfügung, um die beabsichtigte Funktionalität der Integration aufrechtzuerhalten, z. B. kann ein externes System eine Drittanbieter-Datensatz-ID, einen Dateinamen, einen Ordnernamen oder eine ähnliche Kennzeichnung bereitstellen, die dazu dient, einen Datensatz zu identifizieren, der an die Abgedeckten Services gesendet wird. Salesforce kann solche Metadaten erfassen und speichern, um die Produktfunktionalität zu gewährleisten und um bei der Fehlersuche, beim Support und zu Sicherheitszwecken zu helfen. Salesforce bietet angemessenen Schutz für solche Metadaten und behandelt sie in Übereinstimmung mit unserer Datenschutzerklärung. Die Dokumentation zu Sicherheit, Datenschutz und Architektur für die von Salesforce bereitgestellten Services finden Sie in der Vertrauens- und Compliance-Dokumentation.