# Vereinbarung zur Auftragsverarbeitung

Version 2.0

abgeschlossen zwischen

1. Ihnen

(im Folgenden auch **„Auftraggeber"** oder **„Verantwortlicher"** genannt)

einerseits, und

2. Pinpoll GmbH, Hopfengasse 3, 4020 Linz, eingetragen im Firmenbuch des Landesgerichtes Linz zu FN 433631 v

(im Folgenden auch **„Auftragnehmer"** oder **„Auftragsverarbeiter"** genannt)

andererseits

(die unter Punkt 1 und 2 Genannten im Folgenden auch gemeinsam **„Vertragsparteien"** genannt)

wie folgt:

## 1. Präambel

**1.1** Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl 04.05.2016 L 119/1 (im Folgenden auch **„DSGVO"** genannt) gilt ab 25.05.2018 unmittelbar in jedem Mitgliedstaat und ist in all ihren Teilen verbindlich. Zur Durchführung der DSGVO wurde mit dem Datenschutzanpassungsgesetz 2018 das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (BGBl I 2018/24, im Folgenden auch **„DSG"** genannt) beschlossen, welches ebenfalls mit 25.05.2018 in Kraft tritt.

**1.2** Der Verantwortliche und der Auftragsverarbeiter haben gemäß Art 28 DSGVO eine Vereinbarung zur Auftragsverarbeitung abzuschließen. Dieser Verpflichtung wird mit der gegenständlichen Vereinbarung entsprochen.

**1.3** In der gegenständlichen Vereinbarung wird explizit auf die DSGVO als Rechtsgrundlage Bezug genommen. Die entsprechenden Bestimmungen des DSG gelten sinngemäß. Sofern das DSG von der DSGVO abweichende Vorschriften vorsieht, wird explizit darauf hingewiesen.

## 2. Gegenstand

**2.1** Die Inanspruchnahme der von Pinpoll zur Verfügung gestellten Software-Komplettlösungen zum Erheben und Analysieren von Nutzerdaten durch den Auftraggeber erfolgt auf der Grundlage der Nutzungsbedingungen und der Datenschutzerklärung des Auftragnehmers in der jeweils gültigen Fassung, abrufbar unter https://pinpoll.com.

**2.2** Die Vereinbarung bezieht sich auf alle Tätigkeiten, bei denen der Auftragnehmer personenbezogene Daten, die ihm der Auftraggeber zur Verfügung stellt, verarbeitet.

**2.3** Die vom Auftragnehmer erhobenen personenbezogenen Daten ergeben sich aus Punkt 3 der Datenschutzerklärung.

**2.4** Bei den von der Verarbeitung betroffenen Personen handelt es sich einerseits um den Auftraggeber selbst und andererseits um Personen, die Dienste des Auftraggebers in Anspruch nehmen und dadurch vom Einsatz der Tools des Auftragnehmers betroffen sind.

**2.5** Die Art und der Zweck der Datenverarbeitung ergeben sich aus Punkt 3.1 und Punkt 6 der Datenschutzerklärung.

## 3. Dauer

Diese Vereinbarung tritt mit der Erstellung eines Pinpoll-Kontos in Kraft und wird auf unbestimmte Zeit abgeschlossen.

## 4. Rechte und Pflichten des Auftraggebers

**4.1** Der Auftraggeber ist als Verantwortlicher zur Einhaltung der datenschutzrechtlichen Bestimmungen nach der DSGVO bzw. anderen einschlägigen Vorschriften zum Datenschutz verpflichtet. Der Auftraggeber ist insbesondere verpflichtet, die Grundsätze der Datenverarbeitung gemäß Art 5 DSGVO einzuhalten und die Rechte und Ansprüche der Betroffenen, insbesondere nach Art 12 bis 22 DSGVO, zu wahren.

**4.2** Der Auftraggeber hat gemäß Art 28 Abs 3 lit a DSGVO und Art 29 DSGVO ein Weisungsrecht. Der Auftraggeber hat die Weisungen schriftlich zu erteilen.

**4.3** Der Auftraggeber ist berechtigt, die Einhaltung der dem Auftragnehmer nach der DSGVO obliegenden technischen oder organisatorischen Sicherheitsmaßnahmen im Sinne des Punktes 6 durch Übermittlung von geeigneten Nachweisen einzufordern.

## 5. Rechte und Pflichten des Auftragnehmers

**5.1** Der Auftragnehmer ist als Auftragsverarbeiter zur Einhaltung der datenschutzrechtlichen Bestimmungen nach der DSGVO bzw. anderen einschlägigen Vorschriften zum Datenschutz verpflichtet.

**5.2** Der Auftragnehmer stellt sicher, dass der Auftraggeber die den Betroffenen zustehenden Rechte gemäß Art 12 bis 22 DSGVO erfüllen kann. Der Auftragnehmer hat insbesondere geeignete technische und organisatorische Sicherheitsmaßnahmen im Sinne des Punktes 6 zu treffen, um den Auftraggeber bei der Beantwortung entsprechender Anträge von Betroffenen zu unterstützen.

**5.3** Der Auftragnehmer verpflichtet sich, den Auftraggeber bei den zu treffenden Maßnahmen in Bezug auf die Datensicherheit gemäß Art 32 DSGVO, bei gegebenenfalls nötigen Meldungen an die Aufsichtsbehörde gemäß Art 33 DSGVO, bei Benachrichtigungen Betroffener gemäß Art 34 DSGVO, bei der Durchführung von Datenschutz-Folgeabschätzungen gemäß Art 35 DSGVO sowie bei der Abstimmung mit Aufsichtsbehörden gemäß Art 36 DSGVO – nach den ihm zur Verfügung stehenden Informationen – zu unterstützen.

**5.4** Der Auftragnehmer ermöglicht Überprüfungen – einschließlich Inspektionen – durch den Auftraggeber oder einem anderen von diesem beauftragten Prüfer und trägt dazu bei.

**5.5** Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gemäß Punkt 4.2 dieser Vereinbarung gegen die DSGVO oder andere einschlägige Datenschutzbestimmungen widerspricht.

## 6. Technische und organisatorische Sicherheitsmaßnahmen

**6.1** Der Auftragnehmer gewährleistet die Umsetzung der im Rahmen der ordnungsgemäßen Durchführung der Auftragsarbeiten erforderlichen Sicherheitsmaßnahmen. Dies gilt auch für die Inanspruchnahme eines Subauftragsverarbeiters gemäß Punkt 7 dieser Vereinbarung. Der Auftragnehmer bzw. der Subauftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten, die den Anforderungen der DSGVO, insbesondere nach Art 32 DSGVO, genügen (Details sind der Anlage ./1 zu entnehmen).

**6.2** Die erforderlichen technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist der Auftragnehmer berechtigt, alternative adäquate Maßnahmen umzusetzen.

**6.3** Der Auftragnehmer verweist in diesem Zusammenhang insbesondere, aber nicht ausschließlich, auf die Terms und Zertifizierungen in der jeweils aktuellen Fassung seines Subauftragsverarbeiters gemäß Punkt 7.2, abrufbar unter http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=12830 bzw. https://azure.microsoft.com/de-de/overview/trusted-cloud/.

**6.4** Dem Auftraggeber sind die vom Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen bekannt. Der Auftraggeber trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden personenbezogenen Daten ein angemessenes Schutzniveau bieten.

## 7. Subauftragsverarbeiter

**7.1** Der Auftragnehmer ist berechtigt, weitere Auftragsverarbeiter (im Folgenden auch **„Subauftragsverarbeiter"**) zur Verarbeitung von Daten des Auftraggebers heranzuziehen. Der Auftragnehmer haftet für Verschulden des Subauftragsverarbeiters wie für eigenes Verschulden.

**7.2** Der Auftraggeber erteilt hiermit unwiderruflich seine Zustimmung zur Beauftragung von Microsoft Corporation, Redmond, WA 98052-6399 USA, als Subauftragsverarbeiter durch den Auftragnehmer. Die Zustimmung kann widerrufen werden, wenn im Hinblick auf die Beiziehung von Microsoft Corporation als Subauftragsverarbeiter die Voraussetzungen gemäß Art 45 ff DSGVO nicht mehr vorliegen.

**7.3** Der Auftragnehmer informiert den Auftraggeber spätestens 1 (in Worten: ein) Monat vor der geplanten Beauftragung eines weiteren Subauftragsverarbeiters und teilt dem Auftraggeber Name und Anschrift des Subauftragsverarbeiters mit.

**7.4** Der Auftraggeber kann binnen 14 (in Worten: vierzehn) Tagen nach Erhalt der Information gemäß Punkt 7.2 zur Beauftragung des Subauftragsverarbeiters schriftlich Einspruch erheben. In diesem Fall entscheiden der Auftragnehmer und der Auftraggeber über die weitere Zusammenarbeit.

## 8. Löschung von Daten

**8.1** Der Auftragnehmer ist berechtigt, die ihm im Rahmen der Verarbeitung überlassenen personenbezogenen Daten (insbesondere Datenträger und Unterlagen) solange aufzubewahren, wie dies zur Durchführung der jeweiligen Auftragsverarbeitung notwendig ist.

**8.2** Auf Verlangen des Auftraggebers sowie nach Beendigung der gegenständlichen Vereinbarung ist der Auftragnehmer verpflichtet, sämtliche im Zusammenhang mit der Auftragsverarbeitung überlassenen, personenbezogenen Daten (insbesondere Datenträger und Unterlagen) unverzüglich, jedoch spätestens binnen 14 (in Worten: vierzehn) Tagen nach Aufforderung und Weisung des Auftraggebers bzw. nach Abschluss der vertraglich vereinbarten Leistungen, unter Einhaltung der entsprechenden datenschutzrechtlichen Bestimmungen zu löschen bzw. zu vernichten. Nach Durchführung der Löschung bzw. Vernichtung wird Pinpoll dies schriftlich bestätigen.

## 9. Geheimhaltung

**9.1** Die Vertragsparteien, deren Organe, Vertreter, Mitarbeiter oder Erfüllungsgehilfen, verpflichten sich, alle gegenseitig mitgeteilten Vorgaben, Daten, Unterlagen, eigene oder gemeinsame Entwicklungsergebnisse, oder sonstige entwicklungs- oder betriebsbezogenen Informationen, während der Vertragsdauer und nachvertraglich zeitlich unbegrenzt, vertraulich zu behandeln und Dritten nicht mitzuteilen. Die Vertragsparteien verpflichten sich dafür zu sorgen, dass deren Organe, Vertreter, Mitarbeiter oder Erfüllungsgehilfen die zuvor beschriebene Pflichten übernehmen.

**9.2** Geheimzuhalten sind insbesondere

**9.2.1** Tatsachen oder Informationen über Betriebsabläufe;

**9.2.2** Produkte;

**9.2.3** Informationen über Beschaffungsformen.

## 10. Beendigung

**10.1** Diese Vereinbarung wird beendet, wenn das Pinpoll-Konto vom Auftraggeber oder vom Auftragnehmer nach mehr als 12 (in Worten: zwölf) monatiger Nicht-Benützung durch den Auftraggeber im Zuge von Datenbereinigungsmaßnahmen oder im Falle eines schwerwiegenden oder wiederholten Verstoßes gegen die Nutzungsbedingungen gelöscht wird.

**10.2** Beide Vertragspartner können diese Vereinbarung ohne Einhaltung einer Frist auflösen, wenn über das Vermögen des jeweils anderen Vertragspartners ein Insolvenzverfahren eröffnet wird, oder der Antrag auf Eröffnung eines solchen Verfahrens mangels kostendeckenden Vermögens abgewiesen wird oder die Voraussetzungen für die Eröffnung eines solchen Verfahrens oder die Abweisung eines solchen Antrages vorliegen oder der jeweils andere Vertragspartner die Zahlungen einstellt, soweit zwingendes Recht dies zulässt.

**10.3** Beide Vertragspartner können diese Vereinbarung nach Ablauf einer Frist von 2 (in Worten: zwei) Monaten auflösen, wenn:

**10.3.1** der jeweils andere Vertragspartner aus welchen Gründen immer nicht mehr in der Lage ist, diese Vereinbarung zu erfüllen;

**10.3.2** der jeweils andere Vertragspartner nachhaltig gegen seine Pflichten aus dieser Vereinbarung verstößt.

## 11. Anfechtungsverzicht

Die Vertragsparteien verzichten, soweit nach zwingendem Recht zulässig, darauf diese Vereinbarung anzufechten, ihre Anpassung zu verlangen oder geltend zu machen, sie sei nicht gültig zustande gekommen oder nichtig.

## 12. Schlussbestimmungen

**12.1** Jede Änderung, Ergänzung sowie Aufhebung dieser Vereinbarung bedarf der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses. Sofern mündliche Nebenabreden bestehen, gelten diese als aufgehoben.

**12.2** Sollte eine Bestimmung dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen dieser Vereinbarung hiervon unberührt. Anstelle der unwirksamen oder undurchführbaren Bestimmung gilt diejenige wirksame und durchführbare Bestimmung als vereinbart, die den mit der unwirksamen oder undurchführbaren Bestimmung verfolgten wirtschaftlichen Zwecken möglichst nahe kommt. Entsprechendes gilt für die ergänzende Vertragsauslegung.

**12.3** Ausschließlicher Gerichtsstand für alle aus oder in Zusammenhang mit dieser Vereinbarung entstehenden Streitigkeiten ist Linz. Die Vereinbarung unterliegt österreichischem Recht unter Ausschluss von internationalen Verweisungsnormen.

**12.4** Im Zweifel gilt der deutsche Text.

## Anlage ./1 – Technische und organisatorische Sicherheitsmaßnahmen

### TEIL A

In Teil A dieser Anlage wird beschrieben, welche technischen und organisatorischen Sicherheitsmaßnahmen der Auftragnehmer ergreift.

### Vertraulichkeit

In diesem Abschnitt wird beschrieben, welche Maßnahmen der Auftragnehmer ergreift, um den Schutz vor unbefugter Preisgabe von Informationen zu gewährleisten:

- Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Gebäude und Büro durch mehrfaches Versperren und einbruchssichere Türschließsysteme, Dokumentation der Schlüsselvergabe;
- Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch starke Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Verschlüsselung von Datenträgern (FileVault);
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen einschließlich Deaktivierung und Löschung von Konten (insbesondere jene mit Administrationsrechten);

### Integrität

In diesem Abschnitt wird beschrieben, welche Maßnahmen der Auftragnehmer ergreift, um unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten zu verhindern:

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, Virtual Private Networks (VPN) und elektronische Signatur;
- Eingabekontrolle: Protokollierung und Dokumentenmanagement zur Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch;

### Verfügbarkeit und Belastbarkeit

In diesem Abschnitt wird beschrieben, welche Maßnahmen der Auftragnehmer ergreift, um zufällige oder mutwillige Zerstörung bzw. Verlust von Daten zu verhindern:

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Backup-Strategie (sowohl online/offline als auch on-site/off-site), Virenschutz, Firewall, Klimatisierung der Räumlichkeiten, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- Rasche Wiederherstellbarkeit durch hohe Verfügbarkeit;

### Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

In diesem Abschnitt wird beschrieben, welche organisatorischen Maßnahmen der Auftragnehmer ergreift, um ein hohes Datenschutzniveau aufrechtzuerhalten:

- Vereinbarung strenger Geheimhaltungserklärungen mit allen Mitarbeitern;
- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter- Sensibilisierung und Mitarbeiter-Schulungen;
- CRM gestütztes Incident-Response-Management (Ticketing, automatisierte Workflows);

- Auftragskontrolle (vgl. TEIL B): Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen;

## TEIL B

Der Auftragnehmer hat sich darüber hinaus davon überzeugt, dass der Subauftragsverarbeiter Microsoft ausreichende technische und organisatorische Sicherheitsmaßnahmen ergreift. Diese werden In Teil B dieser Anlage beschrieben.

## Vertraulichkeit

In diesem Abschnitt wird beschrieben, welche Maßnahmen unser Subauftragsverarbeiter Microsoft u.a. ergreift, um den Schutz vor unbefugter Preisgabe von Informationen zu gewährleisten.

| Bereich | Praktiken |
|---|---|
| **Physische Sicherheit und Sicherheit der Umgebung** | **Physischer Zugang zu Einrichtungen**<br>Microsoft beschränkt den Zugang zu Einrichtungen, in denen ihre Informationssysteme, die Kundendaten verarbeiten, befinden, auf benannte autorisierte Personen.<br><br>**Physischer Zugang zu Komponenten**<br>Microsoft führt Unterlagen über die eingehenden und ausgehenden Medien, die Kundendaten enthalten, einschließlich Art des Mediums, autorisierte(r) Absender/Empfänger, Datum und Uhrzeit, Anzahl der Medien und Arten von Kundendaten, die sie enthalten. |
| **Zugriffskontrolle** | **Zugriffsrichtlinie**<br>Microsoft führt Unterlagen über Sicherheitsberechtigungen einzelner Personen, die auf Kundendaten zugreifen.<br><br>**Zugriffsautorisierung**<br>Microsoft führt und aktualisiert Unterlagen zu den Mitarbeitern, die für den Zugriff auf Microsoft-Systeme, die Kundendaten enthalten, autorisiert sind.<br>Microsoft deaktiviert Anmeldedaten, die über einen Zeitraum, der sechs Monate nicht überschreiten darf, nicht verwendet wurden.<br>Microsoft benennt diejenigen Mitarbeiter, die berechtigt sind, den autorisierten Zugriff auf Daten und Ressourcen zu gewähren, zu ändern oder zu widerrufen.<br>Wenn mehrere Personen Zugriff auf die Systeme haben, auf denen Kundendaten enthalten sind, stellt Microsoft sicher, dass diese Personen über separate Kennungen/Anmeldedaten verfügen.<br><br>**Geringste Berechtigung**<br>Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur erlaubt, wenn dies erforderlich ist.<br>Microsoft beschränkt den Zugriff auf Kundendaten nur auf die Personen, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen |
| **Inventarverwaltung** | **Inventarisierung**<br>Microsoft pflegt ein Bestandsinventar aller Medien, auf denen Kundendaten gespeichert sind. Der Zugriff auf die Bestände dieser Medien ist Mitarbeitern von Microsoft vorbehalten, die schriftlich zu diesem Zugriff ermächtigt wurden.<br><br>**Handhabung von Beständen**<br>Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur erlaubt, wenn dies erforderlich ist.<br>Microsoft teilt Kundendaten in Kategorien ein, um die Identifizierung zu erleichtern und eine angemessene Beschränkung des Zugriffs auf Kundendaten zu ermöglichen.<br>Microsoft ordnet Beschränkungen für das Drucken von Kundendaten an und verfügt über Verfahren für die Entsorgung von gedruckten Materialien, die Kundendaten enthalten.<br>Mitarbeiter von Microsoft müssen die Genehmigung von Microsoft erhalten, bevor sie Kundendaten auf tragbaren Geräten speichern, remote auf Kundendaten zugreifen oder Kundendaten außerhalb der Einrichtungen von Microsoft verarbeiten. |

## Integrität

In diesem Abschnitt wird beschrieben, welche Maßnahmen unser Subauftragsverarbeiter Microsoft u.a. ergreift, um unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten zu verhindern.

| Bereich | Praktiken |
|---|---|
| **Zugriffskontrolle** | **Integrität und Vertraulichkeit**<br>Microsoft weist ihre Mitarbeiter an, Administrationssitzungen zu deaktivieren, wenn sie Einrichtungen unter der Kontrolle von Microsoft verlassen oder wenn Computer anderweitig unbeaufsichtigt gelassen werden.<br>Microsoft speichert Kennwörter so, dass sie während ihres Geltungszeitraums nicht lesbar sind.<br><br>**Authentifizierung**<br>Microsoft verwendet Verfahren nach Branchenstandard, um Nutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen.<br>Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass die Kennwörter regelmäßig erneuert werden müssen.<br>Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass das Kennwort mindestens acht Zeichen umfassen muss.<br>Microsoft stellt sicher, dass deaktivierte oder abgelaufene Kennungen keiner anderen Person gewährt werden.<br>Microsoft überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf die Informationssysteme zu verschaffen, oder versetzt den Kunden dazu in die Lage.<br>Microsoft unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die beschädigt oder versehentlich offengelegt wurden.<br>Microsoft verwendet Verfahren nach Branchenstandard zum Schutz von Kennwörtern, einschließlich Verfahren, die die Vertraulichkeit und Integrität von Kennwörtern wahren sollen, wenn sie zugewiesen und verteilt werden sowie während der Speicherung.<br><br>**Netzwerkdesign**<br>Microsoft verfügt über Kontrollen, um zu verhindern, dass Personen, die Zugriffsrechte, die ihnen nicht zugewiesen wurden, annehmen, sich Zugriff auf Kundendaten verschaffen, ohne hierfür autorisiert zu sein. |

## Verfügbarkeit und Belastbarkeit

In diesem Abschnitt wird beschrieben, welche Maßnahmen unser Subauftragsverarbeiter Microsoft u.a. ergreift, um zufällige oder mutwillige Zerstörung bzw. Verlust von Daten zu verhindern

| Bereich | Praktiken |
|---|---|
| **Physische Sicherheit und Sicherheit der Umgebung** | **Schutz vor Störungen**<br>Microsoft verwendet unterschiedliche Systeme nach Branchenstandard, um den Verlust von Daten aufgrund von Stromversorgungsausfällen oder Leitungsstörungen zu verhindern. |
| **Kommunikations- und Betriebsmanagement** | **Betriebsrichtlinie**<br>Microsoft führt Sicherheitsdokumente, in denen die Sicherheitsmaßnahmen und die relevanten Verfahren und Verantwortlichkeiten ihrer Mitarbeiter, die Zugriff auf Kundendaten haben, beschrieben sind.<br><br>**Entsorgung von Komponenten**<br>Microsoft verwendet Verfahren nach Branchenstandard, um Kundendaten zu löschen, wenn sie nicht mehr benötigt werden.<br><br>**Verfahren zur Datenwiederherstellung**<br>Microsoft erstellt fortlaufend, jedoch keinesfalls seltener als einmal pro Woche (es sei denn, es wurden in dem Zeitraum keine Kundendaten aktualisiert) mehrere aktuelle Kopien von Kundendaten, von denen Kundendaten wiederhergestellt werden können, und bewahrt diese auf.<br>Microsoft bewahrt Kopien von Kundendaten und Datenwiederherstellungsverfahren an einem anderen Ort auf als an dem Ort, an dem sich die primären Computergeräte, die die Kundendaten verarbeiten, befinden.<br>Microsoft verfügt über bestimmte Verfahren, die den Zugriff auf Kopien von Kundendaten regeln.<br>Microsoft prüft die Datenwiederherstellungsverfahren mindestens alle sechs Monate, mit Ausnahme der Verfahren für Azure-Dienste für die Verwaltung, die alle zwölf Monate geprüft werden. |

| | |
|---|---|
| | Microsoft protokolliert Datenwiederherstellungsmaßnahmen, einschließlich der verantwortlichen Person, der Beschreibung der wiederhergestellten Daten, gegebenenfalls der verantwortlichen Person sowie welche Daten (gegebenenfalls) beim Datenwiederherstellungsverfahren manuell eingegeben werden mussten.<br>Malware<br>Microsoft verfügt über Antimalwarekontrollen, um zu verhindern, dass Malware unbefugten Zugriff auf Kundendaten erhält, einschließlich Malware aus öffentlichen Netzwerken.<br><br>**Grenzüberschreitende Daten**<br>Microsoft verschlüsselt Kundendaten oder versetzt den Kunden in die Lage, Kundendaten zu verschlüsseln, die über öffentliche Netzwerke übertragen werden.<br>Microsoft beschränkt den Zugriff auf Kundendaten in Medien, die ihre Einrichtungen verlassen.<br>Event-Logging<br>Microsoft zeichnet den Zugriff und die Nutzung von Informationssystemen auf, die Kundendaten enthalten, indem die Zugriffs-ID, Zugriffszeit, gewährte oder verweigerte Autorisierung und entsprechende Aktivität registriert wird, oder versetzt den Kunden dazu in die Lage. |
| **Management von Informationssicherheitszwischenfällen** | **Verfahren für die Reaktion auf Zwischenfälle**<br>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 zur Wiederherstellung von Daten.<br>Bei jeder Sicherheitsverletzung, die als „Sicherheitsvorfall" eingestuft wird, muss unverzüglich und in jedem Fall innerhalb von 5 Werktagen eine entsprechende Meldung (wie im obigen Abschnitt „Meldung von Sicherheitsvorfällen") an Microsoft gemacht werden.<br>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.<br><br>**Dienstüberwachung**<br>Die Sicherheitsmitarbeiter von Microsoft prüfen mindestens alle sechs Monate Protokolle, um bei Bedarf Verbesserungsmaßnahmen vorzuschlagen. |
| **Business Continuity-Management** | Microsoft unterhält Notfallpläne für die Einrichtungen, in denen sich Microsoft-Informationssysteme, die Kundendaten verarbeiten, befinden.<br>Der redundante Speicher von Microsoft sowie ihre Verfahren 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. |

## Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

In diesem Abschnitt wird beschrieben, welche organisatorischen Maßnahmen unser Subauftragsverarbeiter Microsoft u.a. ergreift, um ein hohes Datenschutzniveau aufrechtzuerhalten.

| Bereich | Praktiken |
|---|---|
| **Sicherheit im Personalwesen** | **Sicherheitsschulungen**<br>Microsoft informiert ihre Mitarbeiter über relevante Sicherheitsverfahren und ihre jeweiligen Aufgaben. Außerdem informiert Microsoft ihre Mitarbeiter über mögliche Konsequenzen beim Verstoß gegen die Sicherheitsvorschriften und -verfahren. Microsoft verwendet in Schulungen ausschließlich anonyme Daten. |
| **Organisation der Informationssicherheit** | **Verantwortung für die Sicherheit**<br>Microsoft hat einen oder mehrere Sicherheitsbeauftragte bestimmt, die für die Koordination und Überwachung der Sicherheitsvorschriften und -verfahren verantwortlich sind.<br><br>**Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit**<br>Mitarbeiter von Microsoft mit Zugriff auf Kundendaten unterliegen Vertraulichkeitsverpflichtungen.<br><br>**Risikomanagementprogramm**<br>Microsoft hat vor der Verarbeitung der Kundendaten oder der Einführung des Service für Onlinedienste eine Risikobewertung vorgenommen.<br><br>Microsoft bewahrt ihre Sicherheitsdokumente in Übereinstimmung mit ihren Anforderungen an die Aufbewahrung auf, nachdem diese nicht mehr wirksam sind. |