Datenverarbeitungsvereinbarung

Diese Datenverarbeitungsvereinbarung („DPA“) ergänzt die Service-Bedingungen, abrufbar unter https://www.teammeter.com/de/servicebedingungen, die die Nutzung der SERVICE durch den Kunden regeln. Sie legt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen durch den Auftragsverarbeiter fest.
In dieser Vereinbarung ist AGILEVALUE der Auftragsverarbeiter und der in den Servicebedingungen definierte LIZENZNEHMER der Auftraggeber.

§ 1 Gegenstand und Dauer der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen. Der Auftragsverarbeiter darf die Auftraggeber-Daten ausschließlich in der Art, in dem Umfang und zu den Zwecken verarbeiten, die abschließend in diesem Vertrag festgelegt sind. Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer betrifft ausschließlich die nachfolgend abschließend festgelegten Datenarten und den dort bestimmten Kreis der Betroffenen. Jede davon abweichende Verarbeitung von Auftraggeber-Daten ist dem Auftragnehmer untersagt, insbesondere die Datenverarbeitung für eigene Zwecke, es sei denn die Verarbeitung ist im Rahmen der Auftragserfüllung notwendig (z.B. zu Abrechnungszwecken).

1.2 Die Verarbeitung erfolgt für folgende Zwecke:

- Personal- und Team-Entwicklung mit der Software „Teammeter“.

1.3 Die Dauer der Verarbeitung entspricht der Laufzeit des Vertrags, über die Nutzung von Teammeter (Hauptvertrag).

1.4 Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will.

§ 2 Art und Zweck der Verarbeitung

2.1 Die Art der Verarbeitung umfasst die Erhebung, Speicherung, Übermittlung und Löschung von Daten.

2.2 Der Zweck der Verarbeitung ist die Kompetenzentwicklung der Mitarbeiter.

§ 3 Art der Daten und betroffene Personen

Folgende Arten von personenbezogenen Daten werden verarbeitet:

Daten	**Betroffene Personen**	**Aufbewahrung**
Name	Alle	3 Jahre nach Austritt
E-Mail	Nutzer	3 Jahre nach Austritt

Passwort	Nutzer	Nutzer-Lebenszyklus
IP-Adresse	Nutzer	3 Monate
Profilbild	Nutzer	Nutzer-Lebenszyklus
Kompetenzen	Mitarbeiter	3 Jahre nach Austritt
Kompetenz-Bewertungen und Feedback	Mitarbeiter	3 Jahre nach Austritt
Mitarbeiter-Entwicklungspläne	Mitarbeiter	3 Jahre nach Austritt
Schulungszertifikate	Mitarbeiter	3 Jahre nach Austritt

§ 4 Rechte und Pflichten des Verantwortlichen

4.1 Der Auftraggeber ist der Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

4.2 Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

4.3 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

4.4 Der Verantwortliche benennt weisungsberechtigte Personen und informiert den Auftragsverarbeiter bei Fehlern und Problemen in Bezug auf die Verarbeitung.

§ 5 Pflichten des Auftragsverarbeiters

5.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen dieses Vertrags und gemäß den Weisungen des Verantwortlichen.

5.2 Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

5.3 Der Auftragnehmer wird die Datenverarbeitung im Auftrag grundsätzlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchführen. Dem Auftragnehmer ist eine Datenverarbeitung auch außerhalb von EU oder EWR erlaubt, wenn entsprechende Unterauftragnehmer im Drittland unter Einhaltung der Voraussetzungen nach §8 eingesetzt werden und die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind bzw. eine Ausnahme i.S.d. Art. 49 DSGVO vorliegt.

5.4 Der Auftragsverarbeiter ergreift geeignete technische und organisatorische Maßnahmen, um ein angemessenes Schutzniveau der Daten zu gewährleisten. Der zum Zeitpunkt des

Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage1 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

5.5 Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage1 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

5.6 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten nach den Artikeln 32 bis 36 DSGVO.

5.7 Der Auftragsverarbeiter stellt sicher, dass die mit der Verarbeitung befassten Personen zur Vertraulichkeit verpflichtet sind.

5.8 Im Falle eines Verstoßes gegen die gesetzlichen Regelungen informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich.

§ 6 Mitwirkungspflichten des Auftragsverarbeiters

6.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei verschiedenen Aufgaben, wie z.B. bei der Beantwortung von Betroffenenanfragen oder der Erstellung eines Verarbeitungsverzeichnisses.

§ 7 Kontrollbefugnisse des Auftraggebers

7.1 Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und die vertraglichen Vereinbarungen durch den Auftragsverarbeiter jederzeit zu kontrollieren oder durch einen beauftragten Prüfer kontrollieren zu lassen.

7.2 Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

7.3 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 1 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Die Kosten der Vor-Ort-Kontrolle werden vom Auftraggeber übernommen.

§ 8 Unterauftragsverhältnisse

8.1 Der Auftragsverarbeiter nutzt derzeit die folgenden Sub-Auftragsverarbeiter zur Verarbeitung personenbezogener Daten:

Dienstleister	**Daten**	**Zweck**
Amazon Web Services Services EMEA SARL 352 2789 0057 38 Avenue John F. Kennedy, L-1855, Luxembourg	Alle im § 3	Betrieb in der Cloud der Anwendung
Microsoft Ireland Operations Limited Dublin	Authentifizierungsdaten	Authentifizierung mit Microsoft Entra-ID (Optional)
APIDeck Broederminstraat 9 2018 Antwerp, Belgium	Mitarbeitende	Import von Daten aus dem HRIS (Optional)

8.2 Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den nachfolgend genannten Voraussetzungen zulässig.

8.2.1 Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

8.2.2 Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“).

8.2.3 Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen.

8.3 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

8.4 Nicht als Unterauftragsverhältnisse sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne

konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

§ 9 Rechte der betroffenen Personen

9.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Wahrung der Rechte der betroffenen Personen, insbesondere bei Auskunfts-, Berichtigungs- und Löschungsersuchen.

9.2 Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

§ 10 Mitteilungen von Datenschutzverletzungen

10.1 Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

10.2 Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

10.3 Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

§ 11 Ort der Durchführung und der Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich innerhalb der EU.

§ 12 Dauer der Auftragsverarbeitungsvereinbarung

Die Dauer der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ist an die Vertragslaufzeit des Vertrages für die Nutzung von Teammeter zwischen dem Verantwortlichen und dem Kunden gebunden.

§ 13 Haftung

Für die Haftung der Vertragspartner und das Recht auf Schadensersatz gegenüber Dritten wird auf Art. 82 DSGVO verwiesen.

§ 14 Beendigung

14.1 Nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung besteht.

14.2 Eine Löschung ist in geeigneter Weise zu dokumentieren.

14.3 Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

§ 15 Schlussbestimmungen

15.1 Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform.

15.2 Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

15.3 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, so bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

15.4 Dieser Vertrag unterliegt dem Recht des Bundesstaates Deutschlands.

Anlage 1

Wir betreiben ein Informationssicherheitsmanagementsystem (ISMS), das nach ISO 27001 zertifiziert ist.
Die folgenden Maßnahmen verdeutlichen unser Engagement für Informationssicherheit und stellen einen Auszug der von uns implementierten Kontrollen dar.

Zugriffskontrolle

1. Wir wenden das Prinzip der minimalen Rechte an, indem wir administrative Rechte nur an diejenigen vergeben, die sie unbedingt benötigen, und überprüfen diese Berechtigungen regelmäßig.
2. Änderungen der Berechtigungen werden dokumentiert und gemäß dem Vier-Augen-Prinzip genehmigt.
3. Berechtigungen werden im Rahmen des Offboarding-Prozesses entfernt und jährlich auf ihre Gültigkeit überprüft.
4. Unsere Zugriffskontrollrichtlinie schreibt vor, dass Administratoren MFA (Multi-Faktor-Authentifizierung) aktivieren.

Anwendungssicherheit

1. Unsere Anwendung verlangt von den Benutzern, ein Mindestpasswort zu verwenden, und berechnet die Passwortstärke.
2. Die Anwendung verwendet rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC), um sicherzustellen, dass Benutzer nur Zugriff auf die Daten haben, die sie für ihre Rolle benötigen.
3. Wir protokollieren den Zugriff, die Aktualisierung oder das Löschen von Informationen durch Benutzer in der Anwendung. Protokolle werden für 3 Monate gespeichert.
4. Vertrauliche Daten wie Passwörter werden mit sicheren Algorithmen gehasht oder verschlüsselt.
5. Während der Anwendungsentwicklung führen wir Code-Reviews, statische Code-Analysen, automatisierte Tests und Kompartimentalisierungstests durch, um die Vertraulichkeit der Daten zu gewährleisten.
6. Jährliche Penetrationstests werden von einem unabhängigen Experten durchgeführt.

Gerätesicherheit

1. Die Geräte unserer Mitarbeiter werden mit einem Endpunktmanagementsystem verwaltet, um sie durch Festplattenverschlüsselung, Antivirenprogramme, Firewall, Web-Filterung und automatische Patches zu schützen.
2. Die Daten auf zurückgegebenen Geräten werden gemäß der Richtlinie NIST 800-88 zur Datenlöschung gelöscht.

Cloud-Infrastruktur

1. Unsere Cloud-Infrastruktur ist in mehrere Konten mit Subnetzen unterteilt, um die Kompartimentalisierung zwischen Entwicklungs-, Test- und Produktionsumgebungen sicherzustellen.
2. Schwachstellen in unserer Cloud-Infrastruktur werden automatisch erkannt und im Rahmen eines Patch-Management-Prozesses behoben.
3. Änderungen in unserem Produktionssystem werden in einem Ticket-Management-System dokumentiert und geprüft.
4. Ein SIEM (Security Information and Event Management) analysiert Anwendungsprotokolle und erkennt anormales Verhalten sowie Sicherheitsvorfälle.
5. Ein Bedrohungserkennungssystem in unserer Cloud-Infrastruktur meldet Eindringversuche und Datenlecks.
6. Produktionsdaten werden anonymisiert, bevor sie in unserer Entwicklungs- oder Testumgebung verwendet werden.

Lieferantenmanagement

1. Wir überprüfen die Sicherheitslage unserer Lieferanten, indem wir ISO 27001-Zertifikate anfordern und sie bitten, Sicherheitsfragebögen auszufüllen.

Datenübertragung

1. Wir sichern die Übertragung von Daten aus unserer Anwendung mit dem HTTPS-Protokoll.
2. Sensible Daten dürfen nicht auf externen Geräten gespeichert, gedruckt oder an nicht autorisierte Orte in der Cloud kopiert werden.
3. Vertrauliche Daten werden nur mit autorisierten Methoden übermittelt; personenbezogene Informationen werden dabei angemessen geschützt, z. B. durch Maskierung oder Verschlüsselung.

Datenschutz

1. Ein Datenregister wird gepflegt, das die Datenverarbeitungsaktivitäten, deren Zweck und die damit verbundenen Risiken dokumentiert.
2. Das Datenregister wird mindestens jährlich überprüft, um sicherzustellen, dass die erhobenen Daten nicht übermäßig und ihrem Zweck angemessen sind.
3. Anwendungsdaten werden nach Ablauf der Aufbewahrungsfrist automatisch gelöscht. Die Durchführung wird von einem Informationsverantwortlichen überprüft.
4. Wir verpflichten uns, Anfragen zu Betroffenenrechten im Zusammenhang mit ihren personenbezogenen Daten innerhalb eines Monats zu bearbeiten.

Backup

1. Backups von Anwendungsdaten werden täglich in der Cloud-Infrastruktur durchgeführt und für einen Zeitraum von 3 Monaten aufbewahrt.
2. Backups werden mindestens einmal jährlich getestet, um sicherzustellen, dass sie im Notfall zuverlässig sind und den Anforderungen der Geschäftskontinuität entsprechen.

Vorfallmanagement

1. Im Rahmen des Geschäftskontinuitätsplans wird jährlich eine Liste mit Katastrophenszenarien und Wiederherstellungsverfahren überprüft.
2. Sicherheitsvorfälle werden mit ihren relevanten Aktivitäten und ihrer Behebung dokumentiert. Verdächtige und bestätigte Sicherheitsvorfälle werden von Sicherheits-, Betriebs- oder Supportmitarbeitern untersucht, und geeignete Schritte zur Lösung werden identifiziert und dokumentiert.
3. Bei bestätigten Vorfällen ergreifen wir angemessene Maßnahmen, um Schäden an Produkten und Kunden oder unbefugte Offenlegungen zu minimieren.

Personal

1. Soweit gesetzlich zulässig führen wir Hintergrund- und Referenzüberprüfungen für neue Mitarbeiter durch.
2. Jeder Mitarbeiter wird über Sicherheitsrichtlinien unterrichtet und unterzeichnet eine Vertraulichkeitsvereinbarung.
3. Jeder Mitarbeiter erhält eine jährliche Schulung zu Sicherheitsbewusstsein und Datenschutz. Entwickler müssen eine Schulung zu Anwendungssicherheit und sicherer Entwicklung abschließen.