

TOPdesk und die Datenschutz-Grundverordnung (DS-GVO)

Einführung

Die Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union (EU) wird die neue EU-weite Datenschutzrichtlinie und ersetzt das alte Bundesdatenschutzgesetz (BDSG). Obwohl sie in vielerlei Hinsicht Neues zu bieten hat, insbesondere in Bezug auf die Rechte der betroffenen Personen sowie die Erhöhung von Bußgeldern, bleibt einiges unverändert. Nachdem die Verordnung im Mai 2016 verabschiedet wurde, begann TOPdesk schnell mit den entsprechenden Vorbereitungen. Wir mussten sicherstellen, dass wir als Auftragsverarbeiter von Kundendaten entsprechend der neuen Verordnung handeln. Unsere Verantwortung als Auftragsverarbeiter entsteht im Allgemeinen durch das Speichern von Kundendaten, die in die TOPdesk-Software eingegeben werden. In diesem Zusammenhang sind Sie (als Kunde der TOPdesk Deutschland GmbH) als Verantwortlicher für Ihre Daten zuständig. Zudem sollte Ihnen bewusst sein, dass Sie überprüfen können, welche Daten in das System eingegeben werden. Wir gehen davon aus, dass Daten der IT-, Facility- und Personal-Abteilung in TOPdesk eingegeben werden können und haben daher entsprechende Sicherheitsprozesse erstellt.

Häufig gestellte Fragen

1. Wird TOPdesk rechtzeitig DS-GVO-konform sein?

Unseren Verpflichtungen als Auftragsverarbeiter unter der DS-GVO werden wir rechtzeitig vor der Frist am 25. Mai 2018 nachkommen.

2. Wie wird TOPdesk DS-GVO-konform?

Als Auftragsverarbeiter müssen wir sicherstellen, dass unsere Verarbeitungssysteme für die Art der zu verarbeiteten Daten ausreichend gesichert sind und nur die tatsächlich benötigten Daten verarbeitet werden. Aus diesem Grund haben wir die Verarbeitung und Speicherung von Daten auf die vereinbarte Vertragsdauer und einen kurzen Zeitraum nach der Vertragskündigung begrenzt. So stellen wir sicher, dass Sie nach Vertragsende eine Kopie der gespeicherten Daten anfordern können. Um unsere Kundendaten zu speichern nutzen wir ausschließlich zertifizierte Rechenzentren und lassen diese nach dem internationalen ISAE 3000 Standard auditieren.

Zusätzlich beschränkt TOPdesk das Ausmaß der Datenverarbeitung darauf, was im Rahmen der angebotenen Services notwendig ist: Hauptsächlich die Speicherung von Daten sowie die Bereitstellung von Beratungs- und Support-Services, die einen begrenzten Zugang zu Ihrer TOPdesk-Datenbank erfordern.

Darüber hinaus stellen wir die Einhaltung von Prozessanforderungen durch unsere Sicherheits- und Datenschutzbestimmungen sicher. Diese umfassen die Schulung von Mitarbeitern, Autorisierungsprozesse, Zugangsfiler, Sicherheitsprozeduren (wie z. B. regelmäßiges Testen und strenge Sicherheitsüberprüfungen) sowie die Verschlüsselung von Daten bei der Übertragung. Die meisten Funktionalitätsanforderungen und Systemvoraussetzungen für eine DS-GVO-konforme Verarbeitung waren bereits aufgrund der vorherigen Datenschutz- und Sicherheitsstandards erfüllt. Wir wollen unsere Sicherheitsstandards stets verbessern. Deshalb lassen wir unsere Sicherheitsmaßnahmen von externen Experten überprüfen, einschließlich ISAE 3000 Audits, regelmäßigen Penetrations- und Schwachstellentests sowie einer Angriffserkennung.

Weitere Informationen über unsere Sicherheitsprozesse können bei uns angefragt werden.

3. Welche Schritte hat TOPdesk unternommen, um die Einhaltung der DS-GVO sicherzustellen?

Vorbereitend auf die DS-GVO-Frist haben wir eine umfangreiche Überprüfung unserer Sicherheits- und Datenschutzbestimmungen vorgenommen. Wir haben eine Datenschutz-Folgenabschätzung durchgeführt, um Probleme frühzeitig zu identifizieren und zu beheben und die fristgerechte Einhaltung sicherzustellen. Wir haben zusätzlich eine sorgfältige Überprüfung der relevanten dritten Auftragsverarbeiter, die wir zur Bereitstellung von Services einsetzen, durchgeführt. Des Weiteren haben wir die, für Mitarbeiter mit direktem Kundenkontakt als auch für alle anderen Mitarbeiter, konzipierte Sicherheits- und Datenschutzbildung überarbeitet, um Sicherheitsrisiken zu minimieren. Außerdem haben wir für TOPdesk eine „Recht auf Vergessen“-Funktionalität entwickelt, die das Löschen oder das geforderte Anonymisieren von Daten ermöglicht.

4. Was sind die wesentlichen Auswirkungen der DS-GVO auf TOPdesk?

Sicherzustellen, dass wir Ihre Daten innerhalb des erlaubten Rahmens verarbeiten, ist der wichtigste Punkt der DS-GVO. Wie bereits angeführt, haben wir jedoch in Bezug auf Kundendaten schon immer eine sehr sorgfältige Herangehensweise gewählt. Wir begrenzen den Zugriff auf sensible Daten. Zudem bieten wir Schulungen für diejenigen, die Zugriff haben, implementieren technische Sicherungen gegen unbefugten Zugang und haben Sicherheitsprozesse erstellt, um die Begrenzungen, die wir im Datenaustausch einsetzen, zu unterstützen. Im unwahrscheinlichen Fall eines Datenlecks verfügen wir über Prozesse, welche die Auswirkungen beschränken und es Ihnen, als Verantwortlicher, ermöglichen, DS-GVO-konform zu reagieren.

5. Wurden beim Erreichen der DS-GVO-Konformität Risiken oder Probleme identifiziert?

Wir haben keine Risiken oder Probleme beim Erreichen der DS-GVO-Konformität festgestellt und rechnen derzeit auch nicht mit neuen Risiken oder Problemen.

6. Wie wird die DS-GVO die Beziehung zwischen Kunden und TOPdesk beeinflussen?

Die Verordnung sollte keinen direkten Einfluss auf die Beziehung zu unseren Kunden haben. Natürlich erwarten wir von Ihnen, dass Sie Ihren Verpflichtungen als Verantwortlicher nachkommen. Dazu kann bspw. zählen, dass der Zweck der Verarbeitung oder die Nutzung eines dritten Verarbeiters an die betroffenen Personen kommuniziert und die benötigte Einwilligung der betroffenen Personen eingeholt werden muss.

Wie kann TOPdesk Kunden bei der Einhaltung der DS-GVO helfen?

Wir empfehlen Ihnen, eine unabhängige juristische Beratung zur Einhaltung der DS-GVO einzuholen. Dieses Dokument ist nicht als Ersatz für eine juristische Beratung zur Einhaltung der DS-GVO zu verstehen. Darüber hinaus sollten sie sich sorgfältig überlegen, welche Daten in das System eingegeben werden. Dadurch stellen Sie sicher, dass dies den relevanten DS-GVO-Bestimmungen entspricht.

Bereits vor Inkrafttreten der Grundverordnung sind in TOPdesk DS-GVO-konforme Funktionalitäten enthalten. Dazu zählen z. B.: Autorisierungskontrollen mittels Stammdatensystem, Berechtigungs- und Filterfunktionalitäten, Löschen von Personendaten und die Möglichkeit, bereits gespeicherte Daten anpassen zu können.

Mithilfe des Asset- und Operationsmanagements von TOPdesk können Sie dokumentieren, wie mit Informationen umgegangen wird. Wenn Sie grafische Übersichten verwenden und Dokumentationen zu Datensätzen hochladen, können Sie Impact-Analysen zu Sicherheitsincidents durchführen, indem Sie visualisieren, wie Ihre Infrastruktur-Komponenten miteinander verknüpft sind.

Über die Know-how-Datenbank im Self Service Portal können Sie Ihren Mitarbeitern und Kunden Ihre Datenschutzinformationen, Bestimmungen und Verarbeitungszwecke zur Verfügung stellen. Mithilfe des Incident- und Problemmanagements richten Sie zusätzlich Standard-Prozesse ein, um Sicherheitsincidents nachzuverfolgen. Außerdem kann in TOPdesk der Zugang zu Informationen eingeschränkt oder nach Modulen gefiltert werden, um sicherzustellen, dass sensible Daten gemäß DS-GVO nur berechtigten Nutzern zur Verfügung stehen. Gerne unterstützen unsere Berater Sie bei der Einrichtung der entsprechenden Prozesse innerhalb von TOPdesk.

7. Kontaktinformationen für weitere Fragen

Wenn sich aufgrund dieses Dokuments Fragen ergeben, wenden Sie sich bitte an Ihren Account Manager oder Berater.

Die Gültigkeit und Richtigkeit dieser Informationen gelten ab 05. April 2018. Obwohl das vorliegende Dokument mit größter Sorgfalt verfasst wurde, übernimmt der Herausgeber keinerlei Haftung für Schäden aufgrund von Fehlern und/oder Unvollständigkeiten der vorliegenden Ausgabe. Dieses Dokument dient zur Information und stellt keine juristische Beratung dar. Es kann durch TOPdesk geändert werden, darf aber nicht ohne schriftliche Genehmigung von TOPdesk durch Andere geändert oder in Umlauf gebracht werden.