Praktische Tipps zur datenschutzkonformen Nutzung von TOPdesk und anderen Applikationen gemäß der Datenschutz-Grundverordnung (DSGVO)

1. Datenumfang und Zweck

Mit TOPdesk unterstützen Sie Ihre Mitarbeiter oder Kunden schnell und einfach. Hierfür ist es bei eingehenden Anfragen häufig erforderlich, bestimmte Daten wie E-Mail-Adressen, Telefonnummern, Anschrift und Kontaktinformationen zu erfassen.

Je nachdem, welche Service-Arten Sie anbieten und welche Beziehung zur betroffenen Person besteht, können sich die Daten, die Sie erfassen müssen, in ihrer Art und Sensibilität unterscheiden. Es empfiehlt sich, genau und transparent zu dokumentieren, wie diese personenbezogenen Daten verwendet werden. So ist jedem ersichtlich, wie diese Daten im weiteren Verlauf genutzt werden. Die TOPdesk Know-how-Datenbank unterstützt Sie dabei, alle sicherheitsrelevanten Prozesse niederzuschreiben und Ihren Bearbeitern anschaulich darzustellen. Zudem erhalten Ihre Mitarbeiter oder Kunden Einblicke in den Umgang mit ihren persönlichen Daten.

2. Einverständnis der betroffenen Person

In vielen Fällen wird TOPdesk zur Unterstützung von Mitarbeitern und Kunden der Organisation eingesetzt. Wenn die Erfassung von personenbezogenen Daten für die Erfüllung eines Vertrages notwendig ist, bei dem die betroffene Person Vertragspartner ist - wie zum Beispiel bei einem Arbeitsvertrag oder einem Kunden-/Lieferantenvertrag - können diese ohne Einverständnis verarbeitet werden. Wenn dies jedoch nicht eindeutig ist, wird ein ausdrückliches Einverständnis der betroffenen Person benötigt.

3. Datenzugangskontrolle

Nur Personen, die ein berechtigtes Interesse an einem zuvor definierten Zweck haben, wird ein Zugang zu sensiblen Daten ermöglicht. In TOPdesk können Sie Berechtigungen definieren und Filter erstellen, um sicherzustellen, dass nur die Personen darauf zugreifen können, die dieses berechtigte Interesse vorweisen können (bspw. HR-Abteilung). Indem Sie in TOPdesk personenbezogene Daten (bspw. Ihrer Mitarbeiter) aus einer Quelle wie z. B. einem Azure Active Directory regelmäßig importieren, können Sie dafür sorgen, dass der Zugang zu TOPdesk immer den Sicherheitsrichtlinien Ihres Unternehmens entspricht. Nur Mitarbeiter mit einem aktiven Active Directory-Benutzerkonto können so auf TOPdesk zugreifen.

Vergessen Sie bitte nicht, Ihre Mitarbeiter im Umgang mit personenbezogenen Daten zu schulen, bevor diese Zugänge zu Anwendungen wie bspw. TOPdesk erhalten. Eine Schulung zu Themen wie „allgemeines Sicherheitsbewusstsein“ sowie „Datenschutz“ bietet dafür eine sehr gute Grundlage. Unsere TOPdesk-Berater helfen Ihnen gerne bei der Erstellung und Durchführung solcher Schulungen.

4. Datenaufbewahrungsrichtlinien

In der Datenschutz-Grundverordnung (DSGVO) werden angemessene Datenaufbewahrungsrichtlinien erwähnt. Das bedeutet, dass es in Ihrer Verantwortung liegt, darüber nachzudenken, wie lange personenbezogene Daten verfügbar sein müssen. Zudem müssen Sie sicherstellen, dass sie im Anschluss unwiderruflich gelöscht werden. Davon nicht betroffen sind gesetzliche Vorschriften. Dadurch soll die potentielle Gefahr, dass personenbezogene Daten durch ein Datenleck unbeabsichtigt nach außen dringen, minimiert werden. Beispielsweise wären ehemalige Mitarbeiter, die das Unternehmen vor 10 Jahren verlassen haben, heute immer noch von einem Datenleck betroffen. Darum wurde in der Datenschutz-Grundverordnung festgelegt, dass „alte" Daten zügig entfernt oder für individuelle Personen unauffindbar gemacht werden sollen.

5. Die Wahl der Tools und Lieferanten

Für die Auswahl der für die Erfassung sensibler Daten verwendeten Tools, ist der Datenschutzbeauftragte eines Unternehmens verantwortlich. Die gewählte Lösung sollte es dem Verantwortlichen ermöglichen, zuverlässig mit personenbezogenen Daten umzugehen. Wenn es sich dabei um eine Cloud-Lösung handelt, schließt das auch die Services ein, die im Rahmen von Managementprozessen erbracht werden bzw. Teil davon sind.
Vergessen Sie nicht, sich bereits bei der Auswahl von Softwarelösungen und Lieferanten über die Verarbeitung von personenbezogenen Daten, die Tool-Implementierung sowie relevante Auditberichte zu informieren. Unser ISAE-3000-Auditbericht erklärt, welche Maßnahmen TOPdesk ergreift, um einen zuverlässigen Service zu bieten. Zur Einsicht in diesen Report kontaktieren Sie bitte Ihren Account Manager.

6. Datenschutzvereinbarungen

Stellen Sie sicher, dass bei der Verwendung von Software as Service (SaaS) eine Datenschutzvereinbarung abgeschlossen wurde. In einer solchen Vereinbarung sollten die Zuständigkeiten der beteiligten Parteien deutlich beschrieben sein. Sie enthält unter anderem eine gemeinsame Vertraulichkeitsvereinbarung, eine Vereinbarung über die Art der Zusammenarbeit im Falle von Datenschutzverletzungen und über den Umgang mit Ihren Daten bei Vertragsende. Sorgen Sie dafür, dass Unterauftragsverhältnisse im Vereinbarungsprozess ebenfalls berücksichtigt werden. TOPdesk hat sich selbstverständlich um die Verträge mit allen beteiligten Parteien gekümmert. Wir nutzen ausschließlich Rechenzentren, die ihre Leistungen entsprechend unserer Kundenverpflichtungen erbringen können. Außerdem wurden Datenschutzvereinbarungen zwischen unseren TOPdesk-Niederlassungen und den jeweils beteiligten Rechenzentren abgeschlossen. Es gibt ein großes Angebot an allgemeinen Vorlagen für Datenschutzvereinbarungen, dennoch sollten Sie Ihren Lieferanten fragen, ob dieser über eine eigene Datenschutzvereinbarung für seine Services verfügt. Diese ist in der Regel speziell auf sein Serviceportfolio zugeschnitten. Verwenden Sie die Vorlage Ihres Dienstleisters. Dies erspart Ihnen Zeit und Arbeit bei der Vertragsabstimmung der Datenschutzvereinbarung. Für unsere Services rund um TOPdesk SaaS bieten wir Ihnen eine Vorlage für die Datenschutzvereinbarung. Ihr Account Manager oder unser Datenschutzbeauftragter kann Ihnen dabei helfen, diese vorzubereiten.

7. Recht zur Überprüfung, Berichtigung und „auf Vergessenwerden“

Die Datenschutz-Grundverordnung hilft betroffenen Personen dabei, sich vor den Handlungen anderer zu schützen. Die Datenschutz-Grundverordnung gibt Ihnen das Recht, zu überprüfen, welche Daten über Sie erfasst wurden. Bei Bedarf können Sie zudem fordern, dass die Daten berichtigt oder sogar aus den Datensätzen gelöscht werden.

Für den Fall, dass entsprechende Anfragen eingehen, sollten Ihre Mitarbeiter wissen, wie sie damit umzugehen haben. Das Self Service Portal legt transparent dar, welche Daten aus welchen Gründen erfasst wurden. In der Know-how-Datenbank ist zudem dokumentiert, welche Arten von Daten erfasst werden und zu welchem Zweck. Darüber hinaus kann sie Arbeitsabläufe erklären und visualisieren, sodass diese sowohl für Bearbeiter als auch Kunden klar definiert sind.

Möchte ein Kollege oder Kunde erfahren, welche Daten Sie über ihn gespeichert haben, können Sie diesem die relevanten Daten anhand der Druck-/Exportfunktionalität in TOPdesk zur Verfügung stellen. Die Korrektur fehlerhafter Daten kann direkt in TOPdesk oder in der Quelle, aus der diese importiert werden, erfolgen. Bestimmte Mitarbeiter Ihrer Organisation können personenbezogene Daten überschreiben, sodass es nicht mehr möglich ist, diese Person zu identifizieren. Durch dieses Vorgehen wird das „Recht auf Vergessenwerden“ sichergestellt.

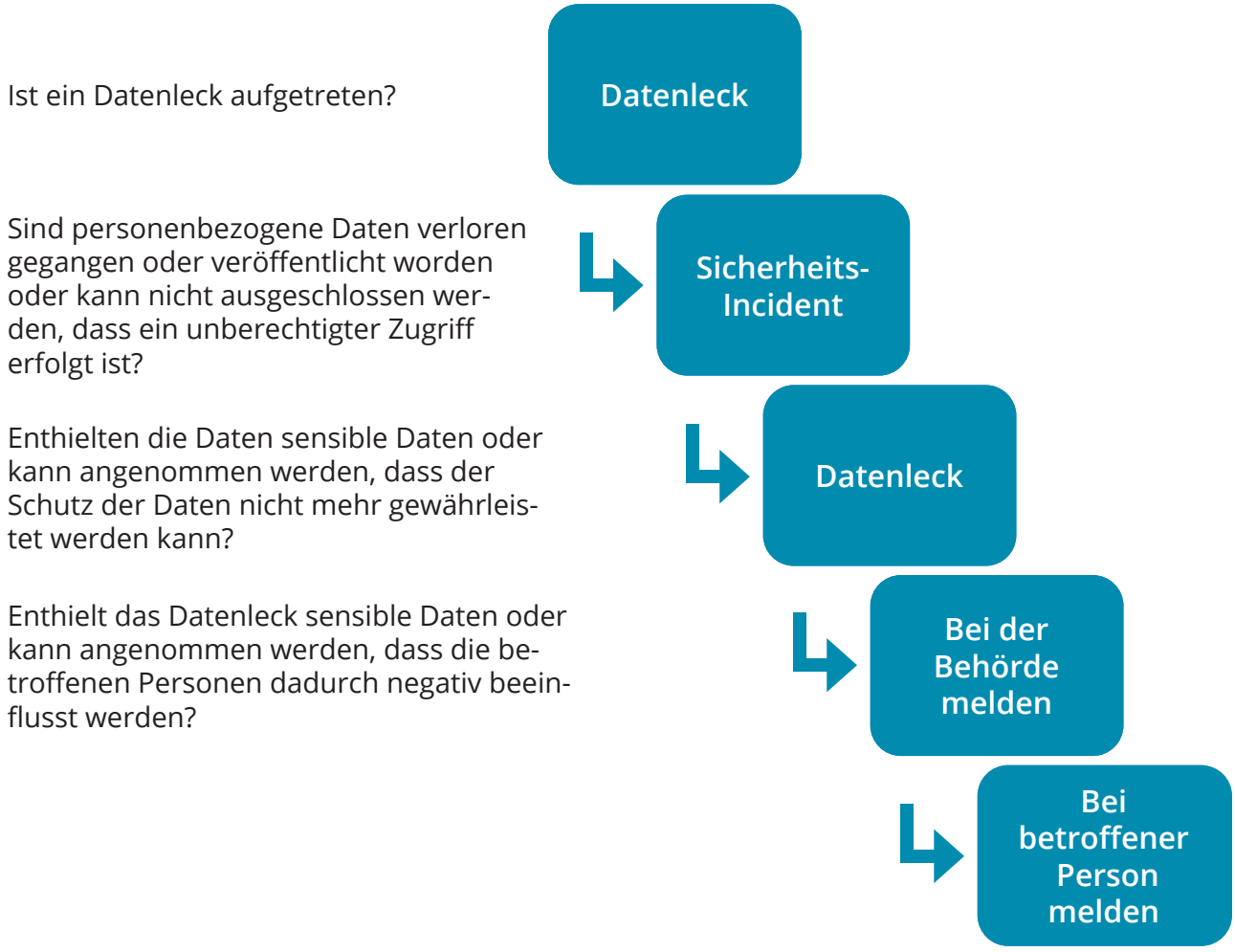
8. Einrichtung eines Prozesses für Sicherheits-Incidents

Vermeiden Sie Stress im Falle eines möglichen Datenlecks, indem Sie bereits im Vorfeld einen Prozess für Sicherheits-Incidents aufsetzen. Im Rahmen dieses Prozesses muss ein entsprechendes Fachwissen vorhanden sein, um die Auswirkungen der Datenschutzverletzung einschätzen zu können. Außerdem müssen ggf. durchzuführende Maßnahmen zur Fehlerbehebung identifiziert und (vorübergehende) Maßnahmen zur Klärung der Situation durchgeführt werden. Im Fall der Fälle hilft es Ihrer Organisation auf einen bereits vorhandenen und etablierten Sicherheitsprozess zurückgreifen zu können, bei dem die jeweiligen Bearbeiter namentlich genannt werden. Ihr TOPdesk Berater kann Ihnen bei der Definition und Umsetzung eines solchen Prozesses in TOPdesk behilflich sein.

Überlegen Sie sich zudem, z. B. eine spezielle E-Mail-Adresse beim E-Mail-Import von TOPdesk sowie ein Formular im Self Service Portal einzurichten, das zur Meldung von Sicherheits-Incidents verwendet werden kann. Anhand von vorgegebenen Kategorisierungen oder Bearbeitergruppen können Sie die Bearbeiter per E-Mail direkt darüber in Kenntnis setzen, dass Ihnen ein neuer Sicherheits-Incident von hoher Priorität eingegangen ist.
Die dem Sicherheits-Incident zugewiesenen Bearbeiter werden bei der Bearbeitung der Datenschutzverletzungen einige Entscheidungen treffen müssen. Da sie den zugrundeliegenden Prozess idealerweise nicht oft durchlaufen müssen, werden ihnen die Verwendung von Self Service-Formularen und die Dokumentation der Abläufe in der Know-how-Datenbank bei der korrekten Bearbeitung des Vorfalls helfen. Außerdem können Sie Ihren Mitarbeitern und Kunden auf diese Weise transparent erklären, wie sie mit solchen Situationen umgehen.

9. Datenlecks melden

In bestimmten Situationen müssen Sie Datenlecks innerhalb von 72 Stunden bei den Behörden und/oder den betroffenen Personen melden. Jedoch kann es dem Image Ihrer Organisation schaden, wenn sich diese Art der Meldungen häufen oder es sich um falsche Meldungen handelt. Daher empfehlen wir, auch diese Abläufe in Ihren Prozess für Sicherheits-Incidents aufzunehmen und vorher zu bestimmen, wer befugt ist, über das Melden von Datenlecks zu entscheiden. Solche Abläufe können folgende Entscheidungsprozesse umfassen:



10. Über (angemessene) Sicherheitsmaßnahmen verfügen

Jede Software, die sensible Daten verarbeitet, unterliegt bestimmten Maßnahmen.
Die Anwendung selbst und die zugrundeliegende Infrastruktur wie Betriebssystem, Datenbank-Server, Netzwerk, etc. müssen sicher konfiguriert und regelmäßig aktualisiert werden. Nur so kann vermieden werden, dass bekannte Schwachstellen für ein Datenleck genutzt werden.

Wenn TOPdesk auf Ihren Servern installiert ist (On-Premises-Variante), müssen sich Personen mit entsprechendem technischen und verfahrenstechnischen Wissen um das Schließen solcher Lücken kümmern. Wenn Sie TOPdesk als SaaS-Variante verwenden, können Sie sich auf das Fachwissen unserer Experten verlassen. Mithilfe von „Continuous Deployment“, Security-by-Design, einem Team von Spezialisten, die sich um die Wartung der SaaS-Instanzen kümmern, stellen wir dies sicher. Zudem führen wir regelmäßige Sicherheitsüberprüfungen durch unabhängige Sicherheitsexperten durch und bleiben so auf dem aktuellen technischen Stand. Dies alles entlastet Sie, sodass Sie sich auf Ihre Mitarbeiter oder Kunden und Ihre angebotenen Services konzentrieren können.

11. Datenlecks beim Datensicherheitsverantwortlichen melden

Falls Sie TOPdesk SaaS nutzen und es sollte ein Datenleck auftreten, verfügen wir über einen Sicherheitsprozess, der dem Leck auf den Grund geht. Die Incidents werden mit der höchsten Priorität behandelt, wodurch Sie als Verantwortlicher innerhalb von 8 Arbeitsstunden, nachdem das Leck bekannt wurde, darüber informiert werden. Selbstverständlich werden Maßnahmen ergriffen, um die Auswirkungen zu reduzieren und die ungewünschte Situation so schnell wie möglich zu beheben. Dadurch wird sichergestellt, dass Ihre Organisation ihren Verpflichtungen aus der Datenschutz-Grundverordnung nachkommt und im Einklang mit Ihrem eigenen Prozess für Sicherheits-Incidents steht.

12. Regelmäßige Sicherheitsüberprüfungen und Audits durchführen, um auf Compliance hin zu überprüfen

Wir empfehlen unseren Kunden, Ihre TOPdesk-Systeme (und alle anderen Systeme mit sensiblen Daten) in regelmäßigen Abständen überprüfen zu lassen. Es spielt keine Rolle, wie gut Ihre eigenen Experten sind - Fehler können passieren. Ein standardmäßiges Admin-Passwort wurde nicht zurückgesetzt, ein Reverse Proxy läuft mit einer veralteten Version, so etwas kann leicht übersehen werden. Ihre wertvollen Daten sind nicht mehr ideal geschützt und Sie riskieren ein Datenleck. Durch Sicherheitsüberprüfungen, die von unabhängigen Experten durchgeführt werden, können solche Schwachstellen rechtzeitig identifiziert und behoben werden. Wenn Sie TOPdesk SaaS verwenden, übernehmen wir diese Aufgabe für Sie. Wir empfehlen unseren Kunden trotzdem, selbst noch einmal Überprüfungen durchzuführen und sind dankbar für die vielen sicherheitsrelevanten Hinweise, die wir jährlich erhalten. Sie geben unseren eigenen Experten wertvolle Tipps bei der Unterstützung von Sicherheitslücken.

Bitte beachten Sie:
Es ist in der Regel kein Problem, den Umgang mit den eigenen Daten zunächst zu definieren und im nächsten Schritt zu dokumentieren. Der Aufwand, der für die Umsetzung dieser Prozesse benötigt wird, kann jedoch leicht unterschätzt werden. Insbesondere alle Beteiligten für das Thema zu sensibilisieren und Bewusstsein für die eigene Rolle zu schaffen, kann sehr **zeitintensiv sein.**