www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT | Dezember 2021

Bild: iStock.com/alvarez

Im Büro, im Homeoffice oder beides? Das Datenschutzniveau muss in allen Konstellationen stimmen.

Hybrid Work regeln und kontrollieren

Neue Arbeitswelt – das ist aus Datenschutzsicht zu beachten

Das neue Arbeiten zwischen Homeoffice und Büro stellt Unternehmen vor vielerlei Herausforderungen. Für Datenschutzbeauftragte ist es umso wichtiger, bei Veränderungen, die die Arbeitssituation der Beschäftigten betreffen, kompetent zu beraten.

Als Unternehmen den Großteil der Arbeitnehmerinnen und Arbeitnehmer im Corona-Jahr 2020 in ihre Homeoffices schicken, hatten wohl die wenigsten vermutet, dass sich daraus eine komplett neue Arbeitswelt entwickeln könnte. Nun – fast zwei Jahre später – sind die anfänglichen Provisorien überwunden, Softwarelizenzen angeschafft, Mitarbeitende mit neuen Kooperationstools vertraut, und die meisten Beschäftigten sind bereit für den nächsten Schritt.

Doch dieser Schritt sieht in zahlreichen Fällen nicht etwa die vollständige Rückkehr in die Büroräumlichkeiten vor. Vielmehr ist aus dem Dauerzustand „Homeoffice" der Wunsch bei vielen Arbeitnehmerinnen und Arbeitnehmern erwachsen, eine Kombination aus mobilem Arbeiten und Arbeiten im Büro als neues Arbeitsmodell einzuführen. Doch hierbei ist auch aus datenschutzrechtlicher Sicht einiges zu beachten. Wichtig sind dabei Regelungen, die sich an veränderte Situationen und an die Unternehmens- wie Mitarbeiterbedürfnisse anpassen lassen – und dieser Bedarf besteht derzeit ja leider ständig.

WICHTIG

Der Arbeitgeber bleibt Verantwortlicher im Sinne von Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO). Er muss daher sicherstellen, dass die Beschäftigten sowohl im Büro als auch im Homeoffice datenschutzkonform arbeiten. Ihn trifft die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO, d.h. er muss nachweisen, dass er die datenschutzrechtlichen Vorschriften einhält. →

Editorial

Ricarda Veidt, Chefredakteurin

Der Datenschutz-PRAXIS-Adventskalender

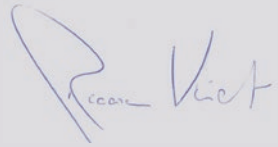
Liebe Leserin, lieber Leser! Was hatten wir alle miteinander gehofft, dass die Vorhersagen aus dem Sommer nicht zutreffen und uns ein weiterer Corona-Winter erspart bleibt.

Um dem Winter- und Corona-Blues ein wenig entgegenzuwirken, finden Sie ab dem 1. Dezember unter www.datenschutz-praxis.de/adventskalender erstmals einen digitalen Adventskalender. Hinter den Türchen erwartet Sie ein „Best of" der Daten-Schluss-Geschichten, vorgelesen vom „Meister" selbst, Eberhard Häcker, aber auch von vielen weiteren Beteiligten aus dem Autoren-, Redaktions- und Datenschutzteam.

Sie wollten schon immer einmal Oliver Schonschek oder Dr. Eugen Ehmann lauschen? Kein Problem, klicken Sie einfach rein. Hören Sie, was meine Chefin Frau Petroff aus der Geschichte „Wenn der Chef das Unternehmen abschießt" macht oder unsere Setzerin aus der internen Mail für die Ewigkeit („Was lange währt ...").

Wir alle hoffen, Ihnen damit eine kleine Freude zu machen. Eine schöne Advents- und Weihnachtszeit Ihnen und Ihrer Familie!

Herzlichst
Ihre Ricarda Veidt



„Klassiker"	Schutzmaßnahmen
WLAN	Da die Beschäftigten beim mobilen Arbeiten die private Internetverbindung nutzen, muss sichergestellt sein, dass das WLAN-Netzwerk passwortverschlüsselt ist – und zwar mit einem entsprechend sicheren Passwort. Existiert eine Passwortrichtlinie im Unternehmen, sollten die Mitarbeiter nochmals darauf hingewiesen werden.
We are family – aber nicht im Homeoffice	Familienmitglieder dürfen nicht auf Arbeitsmaterialien zugreifen. Das Gleiche gilt für vorhandene Sprachassistenten. Sensible Telefonate sollten nicht in der Öffentlichkeit geführt werden, wo unberechtigte Personen mithören können.
Bildschirmsperre	Bildschirme sind zu sperren, wenn nicht davor gearbeitet wird.
Sichtschutzfolien	Sichtschutzfolien vor den Bildschirmen bieten einen darüber hinausgehenden Schutz.
Löschen von personenbezogenen Daten	Papier mit personenbezogenen Daten oder Unternehmensinterna müssen die beschäftigten Personen datenschutzkonform schreddern – und nicht etwa nicht ausreichend geschreddert in der „normalen" Papiersammlung entsorgen. Idealerweise verzichten die Mitarbeiterinnen und Mitarbeiter ganz drauf, Unternehmensunterlagen auszudrucken.
Abschließbare Schränke	Arbeitnehmer sollten die Möglichkeit haben, Ausdrucke mit personenbezogenen Daten – wenn sich Ausdrucke nicht vermeiden lassen – in einem abschließbaren Schrank oder anderem abschließbaren Behältnis aufzubewahren.

Wichtige Schutzmaßnahmen im Homeoffice

Anforderungen an den Datenschutz und die IT-Sicherheit

Zentral ist beim hybriden Arbeiten: Das Arbeiten außerhalb der Räumlichkeiten des Arbeitgebers findet analog zum Arbeiten in den Räumlichkeiten des Arbeitgebers statt. Das bedeutet, dass die Maßnahmen zum Datenschutz und zur IT-Sicherheit dieselben sind, gleich ob jemand mobil oder im Büro arbeitet.

Datenschutzbeauftragte müssen Einhaltung prüfen

Gleichzeitig ist es Aufgabe von Datenschutzbeauftragten (DSB), zu überwachen, ob sich der Verantwortliche an die Datenschutzvorschriften hält. Das ist derzeit eine große Herausforderung: Wie lässt sich sicherstellen, dass sich die Kolleginnen und Kollegen an die datenschutzrechtlichen Vorschriften halten, wenn eine große Zahl nicht im Büro ist? Wie sollen DSB also prüfen, ob alle auch mobil datenschutzkonform arbeiten? Ein auf den ersten Blick schier unlösbares Problem.

Zentral ist, dass eine Richtlinie, Betriebsvereinbarung oder anderweitige Regelung zum hybriden Arbeiten im Detail

festlegt, welche Regelungen zum Datenschutz die Beschäftigten einhalten müssen, wenn sie mobil arbeiten. Die Mitarbeiterinnen und Mitarbeiter selbst haben dann – im Rahmen des für sie Möglichen – sicherzustellen, dass sie diese Vorgaben einhalten. Das bedeutet beispielsweise:

- Selbstverständlich muss der Arbeitgeber sicherstellen, dass die Firmenlaptops regelmäßig Sicherheitsupdates bekommen. Doch jeder Mitarbeiter ist im Gegenzug dazu verpflichtet, anstehende Softwareupdates nicht zu ignorieren und nicht ständig zu verschieben.
- Der Arbeitgeber muss die Sichtschutzfolie für den Laptop kostenfrei zur Verfügung stellen. Doch der Mitarbeiter ist im Gegenzug dazu verpflichtet, diese dann auch an seinem Firmenlaptop korrekt anzubringen.

Idealerweise stellt eine Regelung zu Hybrid Work auch klar, dass der Arbeitgeber Kontrollrechte hat, wenn die Beschäftigten mobil arbeiten. An dieser Stelle könnte die Regelung ergänzend klarstellen, dass dies auch Kontrollen umfasst, für die der Arbeitgeber andere Personen – wie z.B. den Datenschutzbeauftragten – einsetzt. Das erleichtert es DSB erheblich, ihre Arbeit zu tun, und ermöglicht Kontrollen trotz mobilem Arbeiten.

Form möglicher Kontrollen

Mit Sicherheit lässt sich argumentieren, dass eine Vor-Ort-Kontrolle des oder der Datenschutzbeauftragten in den Privaträumen der Mitarbeitenden unter Einhaltung der Hygienevorschriften vertretbar ist. Allerdings muss diese Art der Kontrolle nicht die Regel sein. Vielmehr besteht auch die Möglichkeit, im Rahmen eines Audits z.B. Fragebögen zu verschicken. Hier können DSB gezielt Punkte wie WLAN, Bildschirmsperre, Einsehbarkeit des Arbeitsplatzes, Möglichkeit von abschließbaren Schränken oder zumindest andere Verschließmöglichkeiten sowie eine allgemeine Beschreibung des Homeoffice-Arbeitsplatzes abfragen.

Betriebsrat einbeziehen

Verfügt das Unternehmen über einen Betriebsrat, ist dieser frühzeitig – d.h. am besten bereits bei der Planung, wie das hybride Arbeiten ausgestaltet sein soll – einzubeziehen. Zu beachten ist insbesondere § 87 Abs. 1 Nr. 14 Betriebsverfassungsgesetz (BetrVG). Danach hat der Betriebsrat bei der „Ausgestaltung von mobiler Arbeit, die mittels Informations- und Kommunikationstechnik erbracht wird" ein Mitbestimmungsrecht.

Um sich ein genaueres Bild zu machen, ist auch ein Videocall eine Möglichkeit. So können sich DSB die Gegebenheiten am mobilen Arbeitsplatz zeigen lassen. Den eigenen Kontrollverpflichtungen nachzukommen, ist also keineswegs unmöglich, nur weil die beschäftigten Personen mobil arbeiten.

Sensibilisierung sicherstellen

Um die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter zu verstärken, ist eine (erneute) Schulung zum Thema Datenschutz – mit Schwerpunkt auf das mobile Arbeiten und die Herausforderungen, die das hybride Arbeiten mit sich bringt – empfehlenswert. Auch wenn es zu einem Datenschutzvorfall kommt, weil etwa der Laptop oder ein anderes wichtiges Dokument plötzlich nicht mehr auffindbar ist, sollten die Beschäftigten stets wissen, welche Meldekette und welche Reaktionszeiten sie einhalten müssen.

Ist „Bring-Your-Own-Device" (BYOD) ein Thema, möchten also die Mitarbeiter ihre privaten Endgeräte beim mobilen Arbeiten verwenden, heißt es, die bekannten Risiken von BYOD abzuwägen: Private Daten und Unternehmensdaten werden vermischt, ohne dass der Arbeitgeber eine Kontrollmöglichkeit hierüber hat. Möchte der Arbeitgeber BYOD gestatten, empfehlen Sie dringend, dies in die Regelungen zum hybriden Arbeiten aufzunehmen und Punkte festzulegen wie Kontrollrechte, Datentrennung etwa mithilfe von Container-Lösungen, regelmäßiges Einspielen von Updates, Installation von Sicherheitssoftware etc.

Achtung bei Verträgen zur Auftragsverarbeitung (AV)

Agiert Ihr Unternehmen als Auftragsverarbeiter im Sinn von Art. 28 DSGVO? Dann empfehlen Sie, unbedingt zu überprüfen, welche konkreten Regelungen die Verträge zur Auftragsverarbeitung in Bezug auf das mobile Arbeiten treffen. Besteht z.B. eine vorherige Genehmigungspflicht durch den Verantwortlichen? Ist das mobile Arbeiten gänzlich ausgeschlossen oder ist es unter bestimmten Voraussetzungen möglich?

Denn letztendlich gilt: Hält der Auftragnehmer die vertraglich vereinbarten technischen und organisatorischen Maßnahmen beim mobilen Arbeiten ein und schließt der Vertrag mit dem Auftraggeber das mobile Arbeiten nicht aus, können die Arbeitnehmer auch mobil arbeiten.

PRAXIS-TIPP

Hier ist es ratsam, ein Audit wie oben beschrieben durchzuführen. So haben Sie als DSB einen Nachweis dafür, dass Sie sich von der Homeoffice-Situation ein Bild gemacht haben.

Schließt ein AV-Vertrag das mobile Arbeiten aus, empfehlen Sie, den Verantwortlichen zu bitten, den Vertrag dahingehend abzuändern, dass ein mobiles Arbeiten unter Berücksichtigung der getroffenen Maßnahmen stattfinden darf. Als Alternative schlagen Sie vor, mit den beschäftigten Personen zu vereinbaren, dass sie die Arbeiten der Auftragsverarbeitung an den „Büro-Tagen" durchführen.

Hierbei empfiehlt es sich – aus Nachweisgründen insbesondere gegenüber dem Vertragspartner –, sich dies vom eigenen Mitarbeiter schriftlich bestätigen →

zu lassen. Nur so können Auftragnehmer bei einer etwaigen Kontrolle durch den Vertragspartner belegen, dass sie die Daten des Verantwortlichen entsprechend seiner Weisung nicht außerhalb der Büroräumlichkeiten verarbeiten.

3G am Arbeitsplatz und dessen Kontrolle

Wie gestaltet sich aber das hybride Arbeiten in den Büroräumlichkeiten nach den aktuellen Entwicklungen konkret aus? Im Gespräch ist derzeit, je nach Corona-Lage bundesweit 3G im Beschäftigtenverhältnis einzuführen. In Bayern gilt z.B. bereits die 3G-Regel am Arbeitsplatz, sobald die dortige Corona-Ampel auf „rot" steht, sich also über 600 COVID-19-Patienten auf bayerischen Intensivstationen befinden.

„3G" bedeutet, dass der Arbeitgeber prüfen muss, ob seine Arbeitnehmerinnen und Arbeitnehmer geimpft, genesen oder getestet sind. Wurde bislang aus Datenschutzsicht der Abfrage des Impfstatus stets eine Absage erteilt, so ermächtigt und verpflichtet sogar Art. 6 Abs. 1 Buchst. c DSGVO i.V.m. den Vorschriften der 14. Bayerischen Infektionsschutzmaßnahmenverordnung (BayIfSMV) Arbeitgeber dazu, bei ihren Arbeitnehmern zu prüfen, ob sie einen 3G-Nachweis vorlegen können. Nicht geregelt ist hingegen, dass der Arbeitgeber diese Information dokumentieren oder gar speichern muss. Dennoch wird es sinnvoll sein, einen Nachweis vorlegen zu können, dass sich der Arbeitgeber an die aufgeführten Vorschriften hält.

Das können DSB raten

Wie können Datenschutzbeauftragte dahingehend am besten beraten?

- An erster Stelle sollten die Mitarbeiter über die Regelungen und die daraus entstehende Verpflichtung der Arbeitgeber informiert werden.
- Es muss eine Lösung implementiert werden, wie der Arbeitgeber – unter Wahrung der Datenschutzgrundsätze – die 3G-Prüfung im Betrieb umsetzen kann.
- Um dem Grundsatz der Datenminimierung gerecht zu werden und keinerlei sensible Daten der Mitarbeiter zu speichern, könnten Betriebe alle Mitarbeitenden, die Zutritt zu den Unternehmensräumlichkeiten haben wollen, manuell kontrollieren. Dabei reicht es aus, den „3G-Status" zu überprüfen. Dass dies – gerade bei größeren Unternehmen mit vielen Beschäftigten – keine praxistaugliche Lösung darstellt, liegt auf der Hand.
- Daher sollten Verantwortliche in Betracht ziehen, den Beschäftigten auf einer freiwilligen Basis anzubieten, lediglich zu dokumentieren, dass ein „Impf- oder Genesenenstatus" geprüft wurde – ohne danach zu differenzieren, was der jeweilige Mitarbeiter konkret vorgezeigt hat. Die so erfassten Mitarbeiter haben dann einen längerfristigen Zugang zu den Büroräumlichkeiten. Die negativ getesteten Mitarbeiter erhalten den Zutritt für maximal 48 Stunden, bis sie wieder einen neuen negativen Test vorzeigen müssen.
- Diese Informationen sollten Verantwortliche nicht in der Personalakte ablegen. Denn sobald die Ampel wieder auf „gelb" springt, fallen die Voraussetzungen zur „Corona-Einlasskontrolle" weg. Damit enfällt auch die Rechtsgrundlage. Sollte eine Regelung auf Bundesebene zustande kommen, dürfte Ähnliches gelten. Behalten Sie die Entwicklung in jedem Fall im Auge.

PRAXIS-TIPP

Doris Kiefer ist Rechtsanwältin und leitet als Head of Data Protection das Datenschutzteam eines im SDAX gelisteten E-Commerce-Unternehmens.

Begriffsbestimmungen

Homeoffice: Telearbeit oder mobiles Arbeiten?

Zwar heißt es umgangssprachlich oft „Homeoffice". Dennoch sei an dieser Stelle die rechtliche Unterscheidung zwischen den Begriffen „Telearbeitsplatz" und „mobiles Arbeiten" aufgezeigt.

§ 2 Abs. 7 der Arbeitsstättenverordnung (ArbStättV) definiert ganz genau, was unter der sogenannten „Telearbeit" zu verstehen ist: „Telearbeitsplätze sind vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten, für die der Arbeitgeber eine mit den Beschäftigten vereinbarte wöchentliche Arbeitszeit und die Dauer der Einrichtung festgelegt hat. Ein Telearbeitsplatz ist vom Arbeitgeber erst dann eingerichtet, wenn Arbeitgeber und Beschäftigte die Bedingungen der Telearbeit arbeitsvertraglich oder im Rahmen einer Vereinbarung festgelegt haben und die benötigte Ausstattung des Telearbeitsplatzes mit Mobiliar, Arbeitsmitteln einschließlich der Kommunikationseinrichtungen durch den Arbeitgeber oder eine von ihm beauftragte Person im Privatbereich des Beschäftigten bereitgestellt und installiert ist."

Das, was man heutzutage unter dem Begriff „Homeoffice" versteht, ist mehr als „mobiles Arbeiten" anzusehen. Das mobile Arbeiten ist an keinen festen Arbeitsort gebunden und könnte auch von unterwegs oder einem anderen Ort als dem häuslichen Arbeitszimmer wie einem Café, einem Hotel oder der Wohnung des Lebenspartners stattfinden. Gleich welche Variante Ihr Unternehmen einsetzt bzw. einsetzen will: Aus datenschutzrechtlicher Sicht müssen beide Varianten Kunden- und Mitarbeiterdaten ausreichend schützen.

Bild: iStock.com/DNY59

Aktuelle Studien zeigen, dass neun von zehn Unternehmen Opfer von Diebstahl, Spionage oder Sabotage geworden sind. Unternehmensdaten stehen dabei im Fokus der Kriminellen.

„Kronjuwelen" schützen

Klassifikation von Daten und Umgang mit Informationen

Jedes Unternehmen, das personenbezogene Daten verarbeitet, muss diese Informationen mit geeigneten technischen und organisatorischen Maßnahmen schützen. Die Daten systematisch zu klassifizieren, kann diesen Prozess strukturieren und vereinfachen.

Wollen Unternehmen Maßnahmen ergreifen, um die eigenen Daten und Informationen zu schützen und (Cyber-)Kriminellen den Zugriff darauf zu verwehren, müssen sie in einem ersten Schritt herausfinden, welche Unternehmensinformationen von besonderem Wert sind. Das gilt nicht nur, aber auch für die personenbezogenen Daten. Gleichzeitig ist es wichtig zu wissen, von welchen Cyber-Risiken das eigene Unternehmen tatsächlich betroffen ist.

Inventur der vorhandenen Informationen

Daher steht in der Regel zunächst eine Art „Inventur" an, um einen Überblick über die Daten und Informationen zu gewinnen, die im Unternehmen vorhanden sind. Nur so ist es möglich, die sogenannten „Kronjuwelen" zu identifizieren, die für das eigene Geschäft sowie für die kritischen Unternehmensprozesse und Betriebsabläufe unverzichtbar sind. Derartige Daten und Informationen müssen den höchsten Schutz genießen.

Die enormen Datenmengen, die in Unternehmen vorhanden sind und immer weiter anwachsen, machen diese „Inventur" zu einer Herausforderung. Mit diesem rasanten Wachstum gehen neue Herausforderungen einher: Laut Global Data Protection Index des IT-Konzerns Dell Technologies glaubt die große Mehrheit der Unternehmen, dass die aktuell eingesetzten Datensicherheitslösungen den zukünftigen Geschäftsanforderungen nicht mehr gerecht werden (siehe https://ogy.de/protection-index).

Dazu erschweren es unstrukturiert vorliegende Daten, den Überblick über alle Informationen zu bewahren und genau die Information zu finden, die im Moment benötigt wird. Im Gegensatz zu den strukturierten Daten, die in einer immer gleichen Struktur und gleichem Format verfügbar sind, lassen sich unstrukturierte Daten nicht von einfachen Algorithmen oder Anweisungen verarbeiten.

Glücklicherweise gibt es für diese Herausforderungen Lösungswege, die Datenschutzbeauftragte im Rahmen einer Schulung oder ihrer Beratungstätigkeit vorstellen sollten. Mit einer sinnvollen Strategie zur Informationsklassifizierung lassen sich sowohl unstrukturierte Daten sortieren und bewerten als auch Umgangsregelungen definieren, um die Informationen – je nach Schutzbedarf – praktikabel abzusichern.

Die Informationsklassifizierung

Der Begriff „Informationsklassifizierung" bezeichnet einen Prozess, bei dem Daten in verschiedene Kategorien eingeordnet werden.

- Ziel ist zum einen, die Informationen möglichst effizient nutzen zu können, sie also schnell auffinden und einsetzen zu können.
- Zum anderen geht es darum, besonders kritische oder wichtige Unternehmensinformationen mit den richtigen Schutzmaßnahmen abzusichern.

Die Informationsklassifizierung hat demnach große Schnittmengen mit dem Risikomanagement. Das wirkt sich wiederum auf die Informationssicherheit, die IT-Sicherheit und die Compliance aus.

Vertraulichkeitsklassen

Eine Klassifizierung der vorhandenen Unternehmensinformationen bezüglich ihres Werts bzw. des Vertraulichkeitsgrads ist notwendig, um eine geeignete Risikobeurteilung durchführen und Umgangsregeln definieren zu können. →

Vertraulichkeitsklasse	Beschreibung	Beispiele
Öffentlich	Öffentliche Informationen sind für alle Interessierten, Mitarbeitenden, Kunden, Geschäftspartner und Medien frei verfügbar.	– Informationen auf dem Internetauftritt des Unternehmens
Intern	Interne Informationen sind in der Regel Informationen, die einem größeren Mitarbeiterkreis zugänglich, jedoch nicht für Außenstehende bestimmt sind.	– interne Kommunikation wie üblicher Schriftverkehr per E-Mail – interne Regelungen wie Richtlinien, Rundschreiben, Anweisungen, Organisationspläne
Vertraulich	Vertraulich sind in der Regel alle Informationen, die für den technischen oder finanziellen Erfolg einzelner Unternehmensbereiche von Bedeutung sind. Insbesondere sind dies alle Informationen, deren Kenntnis für Mitbewerber von Wert sein kann.	– vertrauliche Kommunikation (wie E-Mail) – Vertragsentwürfe, Verträge und Vereinbarungen mit entsprechendem vertraulichem Inhalt – Entwicklungs- und Konstruktionsunterlagen – Personaldaten
Streng vertraulich/geheim	Dies sind üblicherweise Informationen, die für den Erfolg und das Weiterbestehen von Unternehmensbereichen oder des ganzen Hauses von größter Bedeutung sind.	– Firmenstrategien – Forschungs- und Entwicklungsprojekte, Rezepturen, Kunden-, Umsatz- und Preislisten, Kundenlistungen, Kalkulationen und Kostenrechnungen – Informationen über Produktionsverfahren und Innovationen – bisher nicht veröffentlichte Produkt- und Entwicklungspläne

Überblick über die Vertraulichkeitsklassen. Die Beispiele sind nicht abschließend und können im Einzelfall eine andere Einstufung erfordern.

Üblich ist ein Klassifizierungsschema, das die Vertraulichkeitsklassen öffentlich, intern, vertraulich und streng vertraulich/geheim kennt (siehe Tabelle oben). Basierend auf der Vertraulichkeitsklasse definieren sich die Umgangsregeln, wie die beschäftigten Personen die jeweiligen Informationen

- kennzeichnen,
- verteilen,
- übertragen,
- speichern und
- löschen/vernichten müssen.

Warum das alles? Datenschutz, ISMS & GeschGehG

Nur diejenigen Unternehmen, die definiert haben, welche personenbezogenen Daten wie besonders zu schützen sind, welche Informationen wie zu löschen sind und welche Informationen mit besonders restriktiven Zugriffsmöglichkeiten zu versehen sind, haben dafür gesorgt, dass die Beschäftigten den Datenschutz im Geschäftsalltag beachten.

Informationen in Vertraulichkeits- bzw. Schutzklassen einzuteilen, ist zudem eine der maßgeblichen Aktivitäten, wenn es darum geht, ein Informationssicherheitsmanagementsystem (ISMS) einzuführen. Die Informationsklassifizierung verfolgt dabei immer das Ziel, Sicherheitsvorfälle zu vermeiden, indem Unternehmen regeln, wie die Beschäftigten mit den Informationen umzugehen haben. Darüber hinaus ist sie Basis für eine erfolgreiche Zertifizierung nach ISO/IEC 27001.

Seit 2019 ist der Schutz von Geschäftsgeheimnissen in einem eigenen Gesetz geregelt. Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) hat zum Ziel, Unternehmen vor Spionage durch Wettbewerber zu schützen. Wer z.B. Opfer eines Cyber-Angriffs geworden ist und sich auf ein Geschäftsgeheimnis berufen will, muss vorab „seine Hausaufgaben gemacht haben".

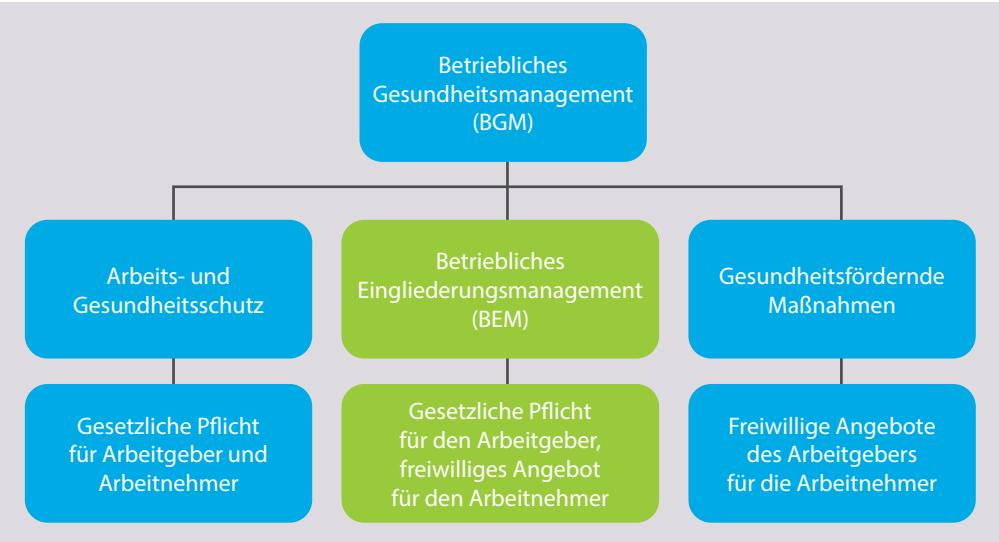
Die Unternehmen müssen im Rahmen des GeschGehG darlegen können, dass sie ihr Know-how, also die kritischen Unternehmensinformationen, durch angemessene Maßnahmen geschützt haben. Hierzu gehört, die Informationen klassifiziert und Maßnahmen etabliert zu haben, um ebendiese Geschäftsgeheimnisse ausreichend zu sichern.

PRAXIS-TIPP

Wie können Unternehmen den Prozess der Informationsklassifizierung konkret angehen?

- ***Zunächst sollten sie eine Richtlinie zur Klassifikation von und zum Umgang mit Informationen entwickeln. Die Richtlinie definiert die Regeln, auf die sich der Klassifizierungsprozess stützt.***
- ***In einem zweiten Schritt setzen die einzelnen Fachabteilungen als Dateneigner den Klassifizierungsprozess um. Das heißt, sie stufen die Informationen in die jeweilige Schutzklasse ein, die wiederum den Umgang mit der Information regelt. Hier hat es sich als sinnvoll erwiesen, mit den „Kronjuwelen" zu starten, also mit den Informationen, die für das eigene Geschäft unverzichtbar sind.***
- ***Last but not least gehört es zum Prozess, die Beschäftigten bezüglich der Richtlinie und des Prozesses zu sensibilisieren und zu schulen.***

Markus Vollmuth ist Informationssicherheitsberater bei der atarax Unternehmensgruppe, einem Dienstleister für strategische Unternehmenssicherheit und Haftungsmanagement. Seine Schwerpunkte sind Informationssicherheit und Datenschutz.



Die einzelnen Bausteine des betrieblichen Gesundheitsmanagements. Das BEM ist einer dieser Bausteine.

Beschäftigtendatenschutz

Datenschutz im betrieblichen Eingliederungsmanagement

Wie ist ein Betriebliches Eingliederungsmanagement (BEM) strukturiert? Welche Herausforderungen entstehen daraus für Unternehmen aus Sicht des Datenschutzes? Und welche konkreten Überwachungsaufgaben ergeben sich damit für Datenschutzbeauftragte (DSB)?

Die Gesundheit der Beschäftigten in Unternehmen hat in den letzten Jahren zunehmend an Bedeutung gewonnen. Viele Unternehmen haben erkannt, dass die Herausforderungen der modernen Arbeitswelt im Zusammenspiel mit dem demografischen Wandel zu einer zunehmenden Nachfrage an qualifizierten Fachkräften führen. Diese sind aber nur in einem begrenzten Maß vorhanden.

Vor diesem Hintergrund beschäftigen sich viele Unternehmen umfassend mit den Möglichkeiten eines betrieblichen Gesundheitsmanagements (BGM). Es fasst sowohl die betrieblichen Pflichten als auch die freiwilligen Maßnahmen zusammen (siehe dazu Fackeldey, Datenschutz im betrieblichen Gesundheitsmanagement, Datenschutz PRAXIS 11/2020, S. 7–10).

Warum ist das betriebliche Eingliederungsmanagement wichtig?

Ein Eingliederungsmanagement als Baustein im Rahmen des betrieblichen Gesundheitsmanagements bietet den Arbeitgebern die Möglichkeit, sich mit ihren Beschäftigten und deren Erkrankungen auseinanderzusetzen. Da es häufig zu Erkrankungen kommt, die auf das jeweilige Arbeitsverhältnis bzw. die vorhandenen Arbeitsbedingungen zurückzuführen sind, besteht über ein BEM die Möglichkeit, seine Beschäftigten gesund und arbeitsfähig zu halten.

Arbeitsunfälle, Überbelastungen, Stressreaktionen, Konflikte unter Kolleginnen und Kollegen und vieles mehr lassen sich durch ein BEM feststellen und konkret bewerten. Geeignete Maßnahmen wiederum können dabei helfen, die Arbeitsbedingungen für die Beschäftigten zu verbessern und Krankheitszeiten zu reduzieren.

Welche Pflichten haben Unternehmen?

Um die gesellschaftliche Bedeutung des BEM zu betonen, hat der Gesetzgeber mit § 167 Abs. 2 Neuntes Buch Sozialgesetzbuch (SGB IX) eine rechtliche Struktur zum BEM geschaffen und folgende Verpflichtung für Unternehmen festgeschrieben: →

Individuelle Maßnahmen nötig

So individuell der Mensch und sein Arbeitsplatz sind, so individuell können auch die Maßnahmen im Rahmen eines BEM sein. Bei einer Küchenhilfe kann z.B. eine Stehhilfe bereits dazu beitragen, ihre Bandscheibenprobleme im Arbeitsalltag in den Griff zu bekommen. Einem Koch kann ein kontrastreiches Schneidebrett dabei helfen, trotz Seheinschränkungen verlässlich Lebensmittel zu schneiden. Einer Telefonistin kann der Einsatz eines Headsets helfen, die einseitige körperliche Belastung zu kompensieren. Es sind nicht immer nur teure und umfassende Maßnahmen notwendig, um ein erfolgreiches BEM durchzuführen. In vielen Fällen reichen kleinere Anpassungen, um die Belastungen am Arbeitsplatz zu verringern.

„Sind Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig, klärt der Arbeitgeber [...] mit Zustimmung und Beteiligung der betroffenen Person die Möglichkeiten, wie die Arbeitsunfähigkeit möglichst überwunden werden und mit welchen Leistungen oder Hilfen erneuter Arbeitsunfähigkeit vorgebeugt und der Arbeitsplatz erhalten werden kann (Betriebliches Eingliederungsmanagement)."

Um diesen gesetzlichen Vorgaben gerecht werden zu können, sind Unternehmen dazu verpflichtet, Überwachungsstrukturen aufzubauen und regelmäßig diesbezügliche Daten zu verarbeiten. Hierbei verarbeiten sie in der Regel neben den konkreten Arbeitsunfähigkeitszeiten zusätzlich den Namen und ggf. weitere Daten mit Personenbezug, z.B. die Personalnummer.

Welche Rechtsgrundlagen lassen sich für die Datenverarbeitung heranziehen?

Erforderlich für Beschäftigungsverhältnis & rechtliche Verpflichtung

Die Verarbeitung dieser Daten ist erforderlich, um die gesetzlich definierte Sechs-Wochen-Frist zu berechnen und dem Auftrag, ein betriebliches Eingliederungsmanagement anzubieten, gerecht werden zu können. Da sich Krankheiten und wiederholte Arbeitsunfähigkeit nicht auf kalendarische Zeiträume begrenzen lassen, ist der zwölfmonatige Beobachtungszeitraum vom Kalenderjahr, also bezogen auf ein Zeitjahr, zu bestimmen. Zusätzlich haben Beschäftigte die Möglichkeit, ihrerseits ein BEM zu beantragen.

Kommt es dazu, dass der Arbeitgeber einer beschäftigten Person ein BEM anbietet, muss er hierzu weitere personenbezogenen Daten verarbeiten, z.B. die Adressdaten, um ihr die Einladung zu einem Erstgespräch zuzusenden.

Die Rechtmäßigkeit der Verarbeitung dieser Daten durch einen Beauftragten des Arbeitgebers und/oder die Personalabteilung lässt sich in der Regel mit § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG) begründen. Denn es handelt sich grundsätzlich um eine Verarbeitung von personenbezogenen Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, die für dessen Durchführung erforderlich ist.

In Ergänzung ergibt sich die Rechtmäßigkeit der Verarbeitung aus Art. 6 Abs. 1 Buchst. c Datenschutz-Grundverordnung (DSGVO). Denn die Verarbeitung ist erforderlich, um eine rechtliche Verpflichtung zu erfüllen, der der Verantwortliche unterliegt.

Zusätzlich: Einwilligung

Diese Rechtmäßigkeit für die Verarbeitung der personenbezogenen Daten lässt sich jedoch lediglich für die Erhebung der Krankheitszeiten und die Einladung zum Erstgespräch, die sich daraus ergibt, ableiten. Alle Prozessschritte, die sich an das Einladungsschreiben anschließen (Zusage zum Gespräch, Durchführung des Gesprächs, Entwicklung weiterer Prozessschritte etc.), benötigen eine eigene Rechtsgrundlage.

Hierzu dürfte die Einwilligung der beschäftigten Person die beste Grundlage sein. Sie lässt sich in der Regel durch § 26 Abs. 2 BDSG begründen. Tatsächlich müssen Unternehmen ab diesem Zeitpunkt zwei verschiedene Einwilligungen betrachten und ihren Nutzen abwägen:

1. Die „Einwilligung des Beschäftigten zur Teilnahme am BEM", damit er jederzeit „Herr des Verfahrens" bleibt und selbst darüber bestimmen kann, welche Maßnahmen das Unternehmen durchführt, wer in den Prozess eingebunden ist und wie die Abläufe gestaltet sind.
2. Die „Einwilligung in die Verarbeitung der personenbezogenen Daten" bzw. der Gesundheitsdaten im Sinne von Art. 9 DSGVO.

Einwilligung zur Teilnahme am BEM

Die „Einwilligung zur Teilnahme am BEM" ist bei jedem Prozessschritt zu hinterfragen. Denn es können sich im Rahmen des BEM-Verfahrens immer wieder Veränderungen einstellen, z.B. durch neue Ziele oder neue Akteure im Prozess. Um diese Veränderungen zu berücksichtigen, ist es erforderlich, die Einwilligungserklärungen regelmäßig anzupassen bzw. neu zu fassen.

An die „Einwilligung zur Verarbeitung der personenbezogenen Daten" legt das BDSG in § 26 Abs. 2 Satz 1 und 2 sehr konkrete und besondere Maßstäbe in Bezug auf die Freiwilligkeit an. Das betrifft v.a. die Abhängigkeit der beschäftigten Person im Beschäftigungsverhältnis und die Umstände, unter denen sie die Einwilligung

ACHTUNG!

Um ein BEM-Verfahren durchführen zu können, nutzt und verarbeitet der Arbeitgeber personenbezogene Daten sowie sensible und vom Gesetz besonders geschützte Gesundheitsdaten des betroffenen Beschäftigten. Nur wenn der Beauftragte des Arbeitgebers Informationen dazu erhält, was der beschäftigten Person fehlt, kann der ergebnisoffene BEM-Prozess dazu führen, die Ziele des BEM auch im Interesse der beschäftigten Person zu erreichen. Dies darf jedoch nie dazu führen, dass Arbeitgeber die rechtlichen Vorgaben aus der DSGVO und dem BDSG nicht beachten.

erteilt hat. Bei der Bewertung der Freiwilligkeit kann es eine Rolle spielen, dass sich aus der erteilten Einwilligung für den Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil einstellt oder der Arbeitgeber und die beschäftigte Person gleichgelagerte Interessen verfolgen.

Was haben DSB mit dem BEM zu tun?

Informieren

Wie ausgeführt ist es erforderlich, personenbezogene Daten zu verarbeiten, um die gesetzlichen Pflichten aus § 167 Abs. 2 SGB IX zu erfüllen. Vor diesem Hintergrund sollten Datenschutzbeauftragte die betrieblichen Akteure wie das BEM-Team und den Beauftragten des Arbeitgebers umfassend informieren, welche datenschutzrechtlichen Anforderungen sie bei der Verarbeitung der Daten zu beachten haben.

Verzeichnis von Verarbeitungstätigkeiten

Auch empfiehlt es sich, den Prozess des BEM als eigenständige Verarbeitungstätigkeit im Rahmen der Dokumentationen des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO) zu beschreiben. Hierbei sollten Datenschutzbeauftragte den Verantwortlichen unterstützen und beraten.

Beratungsaufgaben bei der Entwicklung und Implementierung eines BEM

Darüber hinaus haben DSB bereits bei der Entwicklung und Implementierung von Prozessen und Abläufen konkrete datenschutzrechtliche Beratungsaufgaben. Betrachtet man die möglichen BEM-Prozesse, verarbeiten Unternehmen personenbezogene Daten besonders im Rahmen der folgenden Eckpfeiler:

- betriebliches Frühwarnsystem aufbauen
- Katalog für Erhebungsinstrumente entwickeln
- Katalog für präventive Maßnahmenentwicklung erstellen
- betriebliche Kommunikation und Öffentlichkeitsarbeit, um alle beschäftigten Personen einzubeziehen
- Präventionsverfahren in die betriebliche Gesundheitspolitik einbinden
- Betriebs- bzw. Dienstvereinbarung entwickeln und abschließen
- Konzept entwickeln zur betriebsnahen Rehabilitation einschließlich Regelungen zur stufenweisen Wiedereingliederung
- Kontakt aufnehmen zu außerbetrieblichen Stellen und Diensten
- Kontakt mit den betroffenen Beschäftigten aufnehmen, sie beraten und unterstützen
- Maßnahmen beantragen
- bei der konkreten Maßnahmenentwicklung beraten und unterstützen, Maßnahmen umsetzen und überprüfen

Aus Sicht des DSB ist es wichtig, darauf zu achten, wie der Arbeitgeber die Prozesse beschreibt und als Leitlinien einführt.

Das BEM-Erstgespräch: Informationspflichten und weitere Prozessschritte

Der Gesetzgeber hat in § 167 Abs. 2 SGB IX eine einseitige Verpflichtung formuliert, die dem Arbeitgeber aufträgt, ein BEM anzubieten. Er stellt es jedoch den Beschäftigten frei, dieses Angebot anzunehmen. Verweigert die zu einen BEM eingeladene beschäftigte Person die Zustimmung, so ist das BEM an diesem Punkt beendet.

Wichtig ist hierbei, dass diese Entscheidung nicht zulasten der beschäftigten Person gewertet werden darf. Dem Arbeitgeber bleibt an dieser Stelle nur die Möglichkeit und die Pflicht, das Angebot zu dokumentieren und die Aufbewahrungsfristen für den Nachweis zu definieren.

Stimmt die beschäftigte Person der Einladung zum Erstgespräch zu, dann ist es geboten, sie im Rahmen des Gesprächs umfassend über die Ziele (Zwecke) und den Ablauf des Verfahrens zu informieren. Wichtig ist hierbei auch, die betroffene Person über die Verwendung ihrer Daten im BEM-Prozess zu informieren (im Sinne von Art. 13 und 14 DSGVO). Da die Vertraulichkeit des Gesprächs und die Bestätigung der weiteren Verarbeitung der im Gespräch benannten Informationen besonders wichtig sind, sollte das Ergebnisprotokoll schriftlich niederlegen, wer welche Informationen aus dem Gespräch weiterverarbeiten darf und an wen der Arbeitgeber ggf. welche Daten weitergeben darf. Jede Veränderung der Ziele im BEM-Prozess sollte in Ergänzung zum Ergebnisprotokoll vereinbart und schriftlich niedergelegt werden.

In der Regel bestehen die vereinbarten Schritte im BEM-Prozess aus der Zusammenarbeit mit verschiedenen inner- und außerbetrieblichen Akteuren, um die ursprüngliche krank- →

PRAXIS-TIPP

Es empfiehlt sich, die „Einwilligung zur Verarbeitung der personenbezogenen Daten" an die „Einwilligung zur Teilnahme am BEM" zu koppeln, da sie beide unabhängig voneinander keine Wirkung haben, und ihre Rechtmäßigkeit regelmäßig zu überprüfen.

WICHTIG

Die BEM-Gespräche stellen keine Krankenrückkehrgespräche dar und sind von diesen klar abgegrenzt.

heitsbedingte Gefährdung des Arbeits- und Beschäftigungsverhältnisses zu beseitigen oder zu mindern.

Im Rahmen des Erstgesprächs sollte der Beauftragte des Arbeitgebers die beschäftigte Person über ihre Rechte aufklären (z.B. über die Möglichkeit, die Einwilligung zu widerrufen), über den Verbleib und die Verwendung der erhobenen Daten informieren, auf das Recht hinweisen, in den BEM-Vorgang Einsicht zu nehmen, und auf das Recht, eine Kopie zu erhalten.

Weitergabe von sensiblen Daten an inner- und außerbetriebliche Akteure

Für den BEM-Prozess empfiehlt es sich, sogenannte Dritte unterschiedlicher Fachrichtungen in den Prozess einzubinden, um ein möglichst optimales Ergebnis für die beschäftigte Person bzw. das Unternehmen zu erreichen. Somit kann es sinnvoll sein, folgende betriebliche Akteure in das BEM-System einzubeziehen:

- Interessenvertretung (Betriebsrat/Mitarbeitervertretung/Personalrat)
- Vertrauensperson für schwerbehinderte Menschen (bei Beschäftigten mit einem Grad der Behinderung von 50 % und mehr)
- Vertrauensperson der beschäftigten Person (soweit von ihr gewünscht)
- Werks- oder Betriebsarzt
- gesetzlicher Vertreter
- Fachkraft für Arbeitssicherheit

Darüber hinaus können externe Akteure den Prozess sinnvoll unterstützen, z.B. Rechtsanwälte, Vertreter der Integrationsfachdienste, der Rehabilitationsträger, der Inklusionsämter u.v.m.

Inhalte müssen vertraulich bleiben

Die Inhalte jedes BEM-Gesprächs sind vertraulich zu behandeln. Alle Beteiligten dürfen sie nur für den jeweiligen definierten Zweck nutzen. Je nachdem, welche Akteure ins BEM eingebunden sind, unterliegen sie bereits aufgrund ihrer beruflichen Stellung einer besonderen Schweigepflicht (z.B. Betriebsarzt), andere sollten hierzu verpflichtet werden. Das ist besonders vor dem Hintergrund wichtig, dass betriebliche Ansprechpartner Kenntnis über Teile der geführten Gespräche erhalten, etwa über Leistungseinschränkungen oder Hilfsmaßnahmen.

Da diese Informationen häufig für die Eingliederung an den alten oder neuen Arbeitsplatz entsprechend den Fähigkeiten der beschäftigten Person wichtig sind, ist ihre Verarbeitung zumeist notwendig. Jedoch muss der Verantwortliche sicherstellen, dass sie nur für diesen konkreten Zweck genutzt werden. Aus diesem Grund sollten die Ergebnisse jedes Gesprächs und die Maßnahmen unter Angabe der jeweiligen Zwecke schriftlich festgehalten werden und ggf. auf einer eigenen, neuen Einwilligung fußen.

Über die Inhalte der Dokumentation stimmt sich der Beauftragte des Arbeitgebers mit der beschäftigten Person ab, d.h. der Arbeitgeber dokumentiert nur Informationen, die die beschäftigte Person gegenüber Dritten preisgeben möchte. Der Umfang reicht von einer Mitteilung über das Erstgespräch bis zu ausführlichen Informationen über die arbeitsrelevanten Folgen der Erkrankung bzw. des Unfalls.

Mögliche BEM-Maßnahmen

In vielen BEM-Fällen ist ein erster Schritt, den Arbeitsplatz der beschäftigten Person zu analysieren und mit ihren Fähigkeiten abzugleichen. Für diesen Vergleich benötigt der Arbeitgeber Informationen – sowohl über die berufliche Tätigkeit als auch über die Leistungsfähigkeit.

Die besondere Herausforderung hierbei ist es, nur die Daten zu verarbeiten, die dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind (Art. 5 Abs. 1 Buchst. c DSGVO). Hilfreiche und erforderliche Daten können sein

- Qualifikationen,
- Stärken sowie
- Ziele und eigene Vorstellungen der beschäftigten Person.

Maßnahmen der betrieblichen Eingliederung sind typischerweise stufenweise Wiedereingliederung, Veränderungen des Arbeitsplatzes, der Arbeitsorganisation, der Arbeitsumgebung oder der Arbeitszeit, Arbeitsversuche und Qualifizierungsmaßnahmen.

Einwilligung regelmäßig überprüfen

Die besondere Herausforderung bei der Umsetzung eines BEM: Für die Rückkehr an den Arbeitsplatz sollen Arbeitgeber und Beschäftigte gemeinsam individuelle Lösungen finden. Bei diesem Verfahren erheben und verarbeiten Unternehmen zwangsläufig viele personenbezogene Daten, u.a. Gesundheitsdaten der Beschäftigten. Auch können sich die Ziele und die dazu erforderlichen Schritte immer wieder verändern. Daher ist es unabdingbar, die erteilte Einwilligung der beschäftigten Person regelmäßig zu überprüfen. Auch können Schweigepflichtentbindungen nötig sein.

Sascha Fackeldey ist Geschäftsführer der Digital Compliance Consulting GmbH. Als DSB und Auditor unterstützt er Unternehmen dabei, Datenschutzprozesse einzuführen.

Bild: iStock.com/Feodora Chiosea

Evaluierung des BDSG

Rechtliche Stellung der DSK

Die „Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder", kurz meist als DSK bezeichnet, verfügt über mehr als zwei Dutzend ständige Arbeitskreise, führt mindestens zweimal im Jahr Sitzungen durch und veröffentlicht viel beachtete „offizielle Entschließungen, Orientierungshilfen und weitere Informationen zum Thema Datenschutz" (so die Internetseite der DSK). Gleichwohl ist sie nirgends gesetzlich verankert und hat keinerlei förmliche Entscheidungsbefugnisse.

Wunsch: verbindliche Beschlüsse

Dies steht in deutlichem Kontrast zu dem Einfluss und dem fachlichen Gewicht, das die DSK hat. Die Mitglieder der DSK haben deshalb „vorgeschlagen, die DSK zu institutionalisieren und deren (Mehrheits-)Beschlüsse für verbindlich zu erklären – sei es mittels einer entsprechenden Bestimmung im BDSG oder sei es per Bund-Länder-Staatsvertrag."

Vorschläge aus der Wirtschaft äußern den „Wunsch nach einer möglichst einheitlichen Rechtsauslegung und Rechtsanwendung durch die Datenschutzaufsichtsbehörden in Bund und Ländern." Teilweise regen sie an, zu diesem Zweck „eine Regelung zur einheitlichen Meinungsbildung der Datenschutzaufsichtsbehörden in das BDSG aufzunehmen."

Grundgesetz müsste geändert werden

Nach Auffassung des Bundesinnenministeriums ist all dies ohne eine Änderung des Grundgesetzes nicht möglich. Sie müsste die Grundlage dafür schaffen, dass die Datenschutzbehörden des Bundes und der Länder in einem gemeinsamen Gremium verbindliche Beschlüsse fassen können. Ohne eine solche Grundlage würde eine entsprechende Vorschrift im BDSG gegen das „Verbot der Mischverwaltung" verstoßen.

Dieses Verbot besagt laut Bundesverfassungsgericht, dass die Verwaltungen des Bundes und der Bundesländer ihre Kompetenzen nicht gemeinsam wahrnehmen dürfen. Durchbrochen werden kann es nur durch eine Ausnahmeregelung im Grundgesetz selbst. Ansonsten stellt es lediglich eine „freiwillige Selbstbindung" dar, wenn die Mitglieder der DSK erklären, sich an die Beschlüsse der Konferenz zu halten.

Quelle: Bericht des Bundesministeriums des Innern, für Bau und Heimat (BMI) zur „Evaluierung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU)2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680", Seite 82. Alle Zitate finden sich auf dieser Seite. Der Bericht (Stand: Oktober 2021; Umfang: 143 Seiten) ist abrufbar unter https://ogy.de/evaluierung-bdsg.

Bei Wechsel der Bank

Neues SEPA-Mandat nötig

Ein Kunde hat ein Lastschriftmandat (SEPA-Mandat) erteilt. Nun wechselt er seine Bank. Seine neue Bank teilt dies dem Unternehmen mit, dem der Kunde das SEPA-Mandat erteilt hat. Viele Unternehmen meinen, damit sei alles erledigt. Dies trifft jedoch nicht zu. Vielmehr muss das Unternehmen den Kunden um ein neues SEPA-Mandat bitten.

Einwilligung erforderlich

Datenschutzrechtlich gesehen ist ein SEPA-Mandat eine Einwilligung. Sie bezieht sich auf die Verarbeitung der personenbezogenen Daten, die im konkreten Mandat enthalten sind. Das sind die Daten der Bankverbindung. Ändert sich die Bankverbindung, handelt es sich um neue personenbezogene Daten. Dies hat zur Folge, dass die betroffene Person neu in die Verarbeitung dieser Daten einwilligen muss.

Quelle: Datenschutzaufsicht Thüringen, 3. Tätigkeitsbericht zum Datenschutz nach der DS-GVO 2020, Seiten 49/50 (Darstellung am Beispiel eines SEPA-Mandats für eine Kommune). Der Bericht ist abrufbar unter https://ogy.de/zaftda-tb-thueringen-2020.

Verkehrsunfall

Weitergabe von Zeugendaten

Die Polizei darf Daten von Zeugen nur mit deren Einwilligung an Unfallbeteiligte weitergeben. Darauf hat die Datenschutzaufsicht Thüringen hingewiesen. Die Polizei in Thüringen erfasst bei Verkehrsunfällen den Namen, die Anschrift und die Telefonnummer von Zeugen auf „Personalienaustauschkarten". Auf Wunsch gab sie diese Daten an die Beteiligten von Verkehrsunfällen weiter. Darüber beschwerte sich ein Zeuge. In der bisherigen Form darf die Polizei diesen Service nicht mehr fortführen. Daten von Zeugen darf sie zwar auch künftig festhalten. Eine Weitergabe der Daten an Unfallbeteiligte ist jedoch nur zulässig, wenn der Zeuge eingewilligt hat. Der Grund: Für eine solche Weitergabe gibt es sonst keine Rechtsgrundlage.

Die Daten von Unfallbeteiligten darf die Polizei dagegen auch künftig an andere Unfallbeteiligte weitergeben. Denn zu einem solchen Datenaustausch untereinander sind alle Unfallbeteiligten ohnehin gesetzlich verpflichtet (siehe § 34 Straßenverkehrsordnung).

Quelle: Datenschutzaufsicht Thüringen, 3. Tätigkeitsbericht zum Datenschutz nach der DS-GVO 2020, Seiten 67/68, https://ogy.de/zaftda-tb-thueringen-2020.

Dr. Eugen Ehmann hat Ende November zum sechsten Mal den Deutsch-amerikanischen Datenschutztag in München, veranstaltet vom vbw, moderiert.

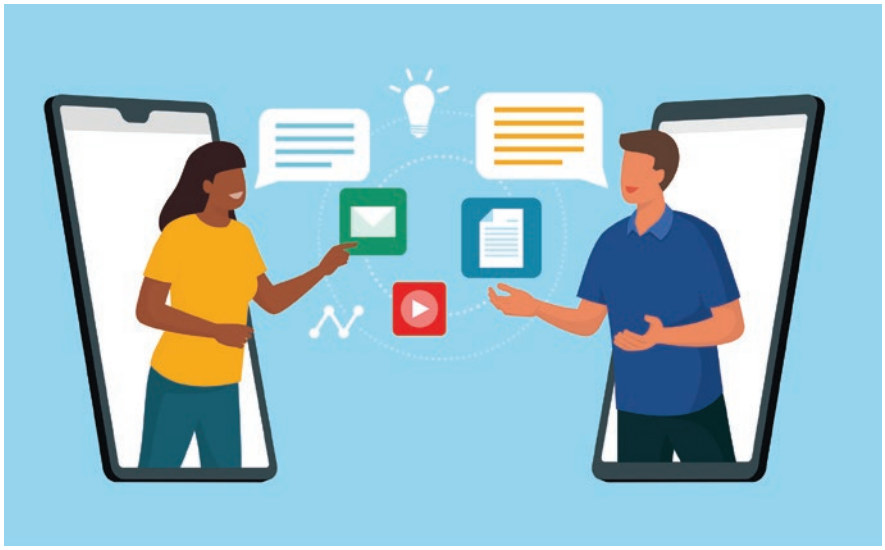


Bild: iStock.com/elenabs

Mit einer anderen Rechtsgrundlage als dem berechtigten Interesse dürfte es schwer werden, den Einsatz von Messengern im Unternehmen zu begründen

Die Vorbereitungsphase

Messenger im Unternehmen: So machen Sie am wenigsten falsch

Viele Beschäftigte wünschen sich, auch im beruflichen Umfeld Messenger nutzen zu können. Dafür müssen aber zahlreiche Punkte im Vorfeld geklärt sein. Zunächst die rechtliche Grundlage. Dann: Was soll der Messenger können, wofür soll er genau zum Einsatz kommen?

Viele Unternehmen verbieten Messenger ausdrücklich. Sie verweisen auf den Datenschutz, aber auch auf das Risiko, dass Verantwortliche zu Diensteanbietern nach dem Telekommunikationsgesetz (TKG) bzw. dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) werden. Inwieweit die Beschäftigten die Verbote einhalten, ließe sich nur durch regelmäßige Kontrollen ermitteln. Doch das machen die wenigsten.

Etliche Unternehmen erlauben es den Beschäftigten aber auch, Messenger zu nutzen. Hier kommt es v.a. darauf an, welche Messenger im Einsatz sind.

Wer die Nutzung von WhatsApp aus Sicht des Datenschutzes untersucht, stellt schnell fest, dass sich schon einige der Grundsätze des Datenschutzes nicht einhalten lassen. Für die Rechtmäßigkeit könnten Unternehmen immerhin noch auf das berechtigte Interesse des Verantwortlichen oder eines Dritten verweisen. Aber spätestens bei der Bedingung, die Rechte und Freiheiten der betroffenen Personen angemessen zu schützen, wird es schwierig. Denn WhatsApp ist nicht für die Nutzung in Unternehmen gedacht. Demzufolge sind auch die rechtlichen Bedingungen nicht zu erfüllen.

ONLINE-TIPP

Inwieweit die Nutzung von WhatsApp im Unternehmen möglich oder unmöglich ist, hat Kirstin Benedikt im Beitrag „WhatsApp auf geschäftlichen Mobilgeräten" in der Ausgabe 09/2018 erläutert (abrufbar unter https://ogy.de/whatsapp-geschaeftlich).

Anders sieht es aus, wenn Unternehmen Messenger wie Signal oder Threema nutzen. Hier sind die rechtlichen Bedingungen anders. Doch nennen Verantwortliche oft als Problem, dass zu wenige Nutzer über diese Messenger verfügen. Daher seien sie kaum praxistauglich.

Entscheidung vorbereiten

Verantwortliche müssen entscheiden, ob sie einen Messenger tatsächlich für erforderlich halten. Denn dann können sie als Rechtsgrundlage Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) verwenden, also das berechtigte Interesse des Verantwortlichen.

Darüber hinaus ist zu klären, welcher Messenger es sein soll. Die meisten werden sich dafür entscheiden, einen vorhandenen Dienst zu verwenden. Es ist jedoch möglich, wenn auch aufwendiger, Messenger-Dienste auf eigenen Servern zu betreiben. Sollen externe Dienstleister zum Einsatz kommen, handelt es sich datenschutzrechtlich um eine Auftragsverarbeitung. Somit ist ein entsprechender Vertrag nötig. Da die meisten Anbieter in einem Drittland, viele davon im unsicheren Drittland USA angesiedelt sind, heißt es, die anspruchsvollen vertraglichen Bedingungen zu betrachten. Dabei weigert sich z.B. WhatsApp, eine Auftragsverarbeitung zu vereinbaren.

Denkbar ist es auch, Messenger-Dienste im Rahmen von Office-Programmen wie Microsoft 365 – in diesem Fall die App „Yammer" – zu nutzen.

Sollen Messenger dazu dienen, mit Kunden zu kommunizieren, ist es sinnvoll, ein Tool zu verwenden, das die Kunden bereits installiert haben. Je sensibler die Daten sind, die übermittelt werden sollen, etwa

Gesundheitsdaten, desto weniger kommen jedoch Standard-Messenger infrage.

Einsatzzwecke und Funktionalitäten planen

Weisen Sie den Verantwortlichen darauf hin, dass er sich vor dem Einsatz eines Messengers grundsätzlich über die Funktionalitäten und die geplanten Einsatzzwecke klar werden muss.

Innerhalb des Unternehmens muss zudem geklärt sein, welche Themen wer wie über den Messenger kommuniziert, wer mitlesen soll, wer auf welche Anfragen zu antworten hat und wie die Antworten dokumentiert werden. Außerdem ist darauf zu achten, dass sich im Rahmen der Arbeitszeit die Ruhezeiten einhalten lassen.

Voraussetzungen für die Erforderlichkeit

Treffen die folgenden Voraussetzungen auch in Ihrem Unternehmen zu, haben Sie eine ganz gute Grundlage, um zu begründen, dass ein Messenger erforderlich ist:

- Der Messenger vereinfacht die Kommunikation innerhalb des Unternehmens.
- Mitarbeiter und Mitarbeiterinnen haben durchblicken lassen, dass sie viele Aufgaben schneller bewältigen könnten, wenn eine reibungslose Kommunikation per Messenger möglich wäre.
- Die Ziele für den Einsatz von Messengern sind definiert.
- Regeln für die Nutzung von Messengern sind entwickelt und angemessen kommuniziert.
- Schulungen zu erforderlichen und zu unterlassenden Messages sind erfolgt.
- Es ist geklärt, wer am Messenger-Dienst teilnehmen soll und wer nicht.
- Es ist geklärt, welche Funktionalitäten der Dienst aufweisen soll.
- Die datenschutzrechtlichen Voraussetzungen sind geklärt.
- Die Mitarbeitenden, die den Messenger nutzen sollen, sind mit den datenschutzrechtlichen Herausforderungen und Lösungen vertraut.
- All diese Anforderungen können in der Summe nicht anders abgedeckt werden.

Zu klärende Datenschutzfragen

Hinsichtlich des Datenschutzes müssen mindestens folgende Fragen geklärt sein:

- Sind die Nachrichten Ende-zu-Ende-verschlüsselt?
- Was geschieht mit Anlagen? Sind sie ebenfalls verschlüsselt? Wenn nicht, wie können beschäftigte Personen sie einfach verschlüsseln? Wie können sie Passwörter und andere Möglichkeiten zur Entschlüsselung sicher übermitteln?
- Welche Metadaten verwendet der Messenger? Wie lassen sich die Metadaten schützen? Wie sollten sich beschäftigte Personen verhalten, damit von ihnen keine unnötigen Profile entstehen?
- Welche Zugriffe auf Kommunikationsgeräte nimmt der Messenger vor? Wertet er beispielsweise Kontaktdaten aus? Und sei es auch nur, um andere Teilnehmer des Messengers darüber zu informieren, dass die beschäftigten Personen nun auch bei diesem Messenger sind? Wie lässt sich dies datenschutzrechtlich begründen?
- Wie lange sollen die Daten im Messenger gespeichert werden?
- Wer erhält Zugriff auf die Messenger, wenn beschäftigte Personen erkrankt sind, ausscheiden oder wenn sie den Messenger nicht mehr nutzen wollen oder dürfen?
- An wen können sich beschäftigte Personen bei Fragen wenden?

Externe Kommunikation mit Messengern

Möchten Unternehmen einen Messenger auch in der externen Kommunikation verwenden, sollten sie vorher folgende Themen abschließend klären:

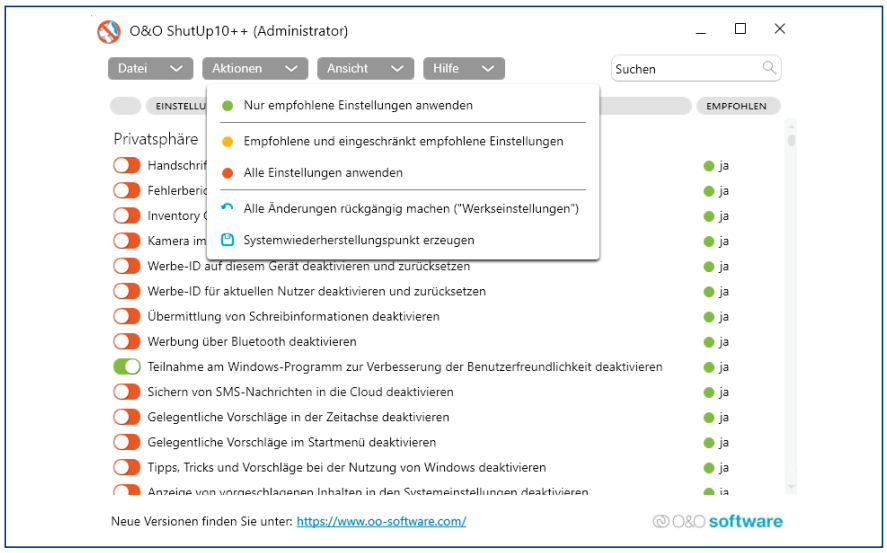
- Welche Informationen oder Serviceangebote für bestimmte Empfänger plant der Verantwortliche zu versenden?
- Welche Informationen kann der Empfänger an das Unternehmen vereinfacht per Messenger übermitteln?
- Sind die rechtlichen Voraussetzungen geklärt: Wer überwacht wie, ob alle Beteiligten sie auch einhalten?
- Verfügen die beschäftigten Personen, die mit dem Messenger arbeiten, über die entsprechende Erfahrung, um zielgerichtet und fehlerfrei zu arbeiten?
- Ist eine lückenlose Kommunikation mit anfragenden oder informationsgebenden Kunden sichergestellt? Ist die Erreichbarkeit gegeben?
- Ist mit beschäftigten Personen geklärt, dass ihre Ängste oder Sorgen entweder berücksichtigt werden oder unbegründet sind?
- Liegt ein „Knigge“ für den richtigen Umgang mit Messengern vor? Hat jemand mit den beschäftigten Personen trainiert?
- Ist sichergestellt, dass die Privatsphäre von Kommunikationspartnern zu jeder Zeit gewahrt ist? Ist eine unzulässige unerwünschte Kontaktaufnahme strikt untersagt und wird sie ggf. sanktioniert?
- Höflichkeit und Zurückhaltung sind in vielen Situationen besser als forsches und anmaßendes Vorgehen. Ist ein entsprechendes Training erfolgt?
- Beschäftigte Personen, die mit Chats arbeiten, dürfen nicht den Überblick verlieren. Ist daher die Zahl der Chats, die sie parallel führen, begrenzt? Zwei, maximal drei sollten die Grenze sein.

Wiederholte Kontrollen, ob die Regeln wirksam sind und die Beschäftigten korrekt mit Messengern umgehen, ist Voraussetzung. Ständige Weiterbildung, v.a. wenn der Messenger neue Funktionalitäten bekommt, ist die Grundlage für den Erfolg.

Ausblick

Wie Sie ganz konkret den „richtigen“ Messenger finden und dabei den Datenschutz sicherstellen, zumindest so weit, dass das Risiko tragbar erscheint, und wie Sie die laufende Betreuung für Datenschutz, Informationssicherheit und Compliance ermöglichen, lesen Sie in einem eigenen Beitrag in einer der nächsten Ausgaben.

Eberhard Häcker kennt das Thema „Messenger“ aus seiner langjährigen Erfahrung als externer DSB. Dabei kann es schon einmal vorkommen, dass er auch nachts über passende Rechtsgrundlagen grübelt.



O&O ShutUp 10++ bremst Windows 10 und Windows 11 beim Schnüffeln aus

Alle Screenshots: Thomas Joos

Technische Maßnahmen

Kostenlose Tools für mehr Datenschutz in Windows

Um den Datenschutz in Windows selbst und bei der Arbeit mit dem System zu verbessern, stehen verschiedene kostenlose Tools zur Verfügung. Mit diesen Werkzeugen lassen sich z.B. Daten einfach verschlüsseln.

Windows 10 und Windows 11 sind bezüglich des Datenschutzes sicher nicht optimal aufgestellt. Es gibt jedoch Möglichkeiten, mit Zusatztools für Verbesserungen zu sorgen. Die hier vorgestellten Werkzeuge sind für den Büroarbeitsplatz und das Homeoffice, aber v.a auch für den privaten Einsatz gedacht. Zentral steuern lassen sie sich nämlich nicht. Doch Administratoren können einiges skripten.

Vor dem Installieren und Ändern: Daten und Einstellungen sichern

Generell gilt: Idealerweise sichern Sie vor den Änderungen das System und dokumentieren unbedingt alle Anpassungen. Windows kann automatisch Systemwiederherstellungspunkte erstellen, wenn Änderungen stattfinden. Dadurch lassen sich die Änderungen bei Problemen rückgängig machen. Die Einstellungen dazu finden sich in Windows 10 und Windows 11 über die Eingabe von „sysdm.cpl“ auf der Registerkarte „Computerschutz“.

Für das Laufwerk C: sollte mit „Konfigurieren“ die Option „Computerschutz aktivieren“ gesetzt werden. Wiederherstellungen zu bestimmten Systemwiederherstellungspunkten lassen sich mit dem Tool „rstrui.exe“ durchführen.

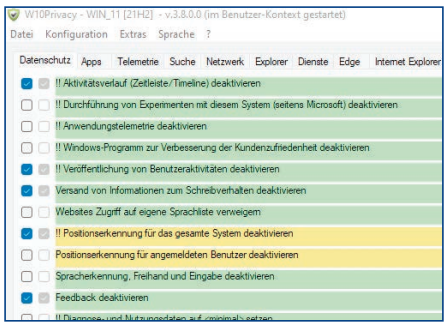
Schnüffelei in Windows 10 und Windows 11 unterbinden: O&O ShutUp und W10Privacy

Bevor Tools zum Einsatz kommen, die den Datenschutz in Windows verbessern, ist es sinnvoll, das Betriebssystem selbst zu optimieren. Das bekannte Tool O&O ShutUp, das bereits in Windows 10 die Datenschnüffelei von Microsoft weitgehend unterbindet, gibt es auch in einer Version für Windows 11. Mit „O&O Shut Up10++“ (www.oo-software.com/de/shutup10) lassen sich mit wenigen Klicks die schlimmsten Spionagefunktionen in Windows 10 und Windows 11 abschalten.

Erfreulich ist, dass das Tool aus einer einzelnen Datei besteht und nicht installiert werden muss. Alle Einstellungen lassen sich dadurch schnell und einfach auf die empfohlene Konfiguration setzen. Die Änderungen können Sie jederzeit rückgängig machen.

Über den Menüpunkt „Aktionen“ können Anwender alle empfohlenen Einstellungen umsetzen, aber auch noch weiter gehen und alle Einstellungen des Tools aktivieren, die den Datenschutz betreffen. Mit Schiebereglern lassen sich verschiedene Einstellungen auch manuell aktivieren oder deaktivieren. Die empfohlenen Einstellungen verbessern den Datenschutz schon deutlich.

Eine Alternative zu O&O ShutUp10 ist das Tool „W10Privacy“ (www.w10privacy.de). Auch W10Privacy muss nicht installiert werden. Der Installationsassistent

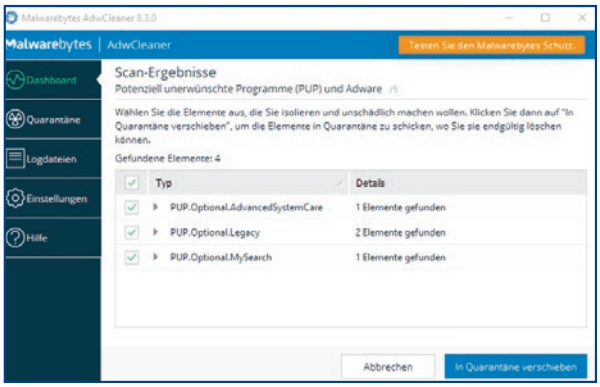


Auch W10Privacy kann in Windows 10 die Datenschutzoptionen verbessern

stellt bei „Installations-Modus“ die Option „Portable Installation“ zur Verfügung. In diesem Fall wird das Tool nur extrahiert. Auch hier gibt es verschiedene Möglichkeiten, den Datenschutz in Windows 10 zu verbessern. Wer Windows 11 nutzt, sollte allerdings auf eine kompatible Version für das neue Betriebssystem warten.

Spionageprogramme von Drittanbietern entfernen: AdwCleaner

Nicht nur Microsoft spioniert die Anwender aus. Viele andere Softwarehersteller installieren mit ihren Anwendungen ebenfalls Spionagefunktionen. Das kostenlose Tool AdwCleaner von Malwarebytes scannt Windows nach Spionagetools, Browser-Hijackern und anderen Schädlingen (https://de.malwarebytes.com/adwcleaner).

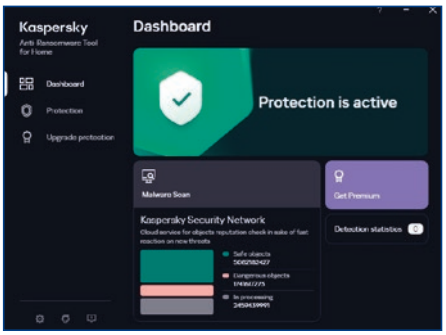


ADwCleaner entfernt Spionageprogramme

AdwCleaner müssen Sie nicht installieren. Direkt nach dem Start durchsucht das Tool mit „Jetzt scannen“ Windows. Nach dem Suchvorgang sehen Sie eine Liste der gefundenen Spionagefunktionen. Mit „In Quarantäne verschieben“ bereinigt AdwCleaner das System.

Schutz vor Ransomware: Kasperskys Anti-Ransomware-Tool

Per erfolgreich eingeschleuster Ransomware übernehmen Kriminelle die Kontrolle über alle Daten, die sich in einem Netzwerk befinden. Mit dem kostenlosen Kasperskys Anti-Ransomware-Tool erhalten Computer einen zusätzlichen Schutz



Kaspersky bietet ein kostenloses Tool für den Schutz gegen Ransomware an

vor Ransomware (www.kaspersky.com/anti-ransomware-tool). Das Tool ersetzt keinesfalls einen Virenscanner, sondern ergänzt die Scanner um Sicherheitsfunktionen für Windows gegen Ransomware. Nach der Installation bindet sich das Tool in Windows ein.

Ist in Windows bereits der überwachte Ordner-Zugriff aktiv, blockiert er das Tool. In diesem Fall muss die IT in der Einstellungs-App von Windows 10/11 bei „Datenschutz & Sicherheit“ über „Windows-Sicherheit“ bei „Ransomware-Schutz“ mit „Ransomware-Schutz verwalten“ und „Blockierungsverlauf“ das Tool von Kaspersky zulassen.

Um das Tool zu verwenden, ist eine kostenlose Registrierung bei Kaspersky notwendig. Wer das nicht will, muss keine echten Daten eintragen, das Tool muss nicht freigeschaltet werden.

Bei allen vorgestellten Tools heißt es übrigens, auf die Lizenzbedingungen zu achten. Nicht jedes ist auch für den Einsatz im geschäftlichen Umfeld kostenlos.

Daten sicher löschen: Secure Eraser & Co.

Wer Dateien in Windows einfach nur löscht, verhindert nicht, dass sie sich wiederherstellen lassen. Wer Daten sicher löschen will, kann auf das Bordmittel-Tool „Cipher“ – erreichbar über die Befehlszeile – setzen. Cipher gehört zum Lieferumfang aller Windows-Versionen. Über den Befehl „cipher /w:<Ordner oder Datei>“ löscht es den Ordner oder die entsprechende Datei und überschreibt anschließend mehrmals den ehemaligen Speicherplatz.

Ein bekanntes Tool für das sichere Löschen ist Secure Eraser (www.ascomp.de, nur für Privatanwender kostenlos). Eine Alternative ist das kostenlose Tool „Sicher Löschen“ (www.softwareok.de/?Microsoft/SicherLoeschen), mit dem sich auch ohne Installation einzelne Dateien sicher löschen lassen. Dazu rufen Sie das Tool auf und ziehen die Dateien per Drag&Drop in die Oberfläche des Programms.

Wer ganze Festplatten löschen will, kann den PC mit einer Live-CD booten und über das System zuverlässig alle Daten löschen. Am besten geeignet dazu ist die Ultimate-Boot-CD (www.ultimatebootcd.com). Um alle Daten zu entfernen, bietet es sich an, z.B. das Tool „CopyWipe“ auf der Ultimate-Boot-CD zu verwenden.

Daten mit Tru Pax verschlüsseln

Um Daten in Windows zu verschlüsseln, gehört VeraCrypt (ehemals TrueCrypt) zu den bekanntesten Tools. Allerdings ist die Lösung komplex in der Bedienung. Das kostenlose „Tru Pax“ (http://ulrich-hanke.de/10/TruPax.html) erstellt VeraCrypt-kompatible Container mit wenigen Mausklicks. Damit lassen sich auch Dateien verschlüsselt auf USB-Sticks speichern.

USB-Sticks mit SecureStick verschlüsseln

Geht es um die Verschlüsselung von USB-Sticks, stellt Microsoft in Windows 10/11 zwar Bitlocker to Go zur Verfügung. Doch nicht jeder möchte auf die Microsoft-Lösung setzen. Das – für Privatanwender – kostenlose Tool SecureStick (www.withopf.com/tools/securstick) kann ebenfalls USB-Sticks verschlüsseln. Der Vorteil des Tools ist, dass es einfach zu bedienen ist.

Thomas Joos hat über 30 Jahre Berufserfahrung als IT-Consultant und Trainer.

Bild: iStock.com/http://www.fotogestoeber.de

Für das Einwilligungserfordernis ist es nicht entscheidend, ob es um personenbezogene Daten geht oder nicht

„Schutz von Endeinrichtungen"

TTDSG: Schärfere Regeln fürs Online-Tracking

Mit § 25 TTDSG tritt am 01.12.2021 die Regelung zum Schutz der Privatsphäre von Endeinrichtungen in Kraft. Diskutiert wurde diese Vorgabe unter dem Schlagwort „Cookie-Regelung". Doch Achtung: Zwar geht es auch um den Einsatz von Cookies. Es beschränkt sich aber nicht darauf.

§ 25 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) regelt in Abs. 1 Satz 1 die „Speicherung von Informationen in der Endeinrichtung des Endnutzers oder [den] Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind". Er erfasst damit u.a. das viel diskutierte Setzen und Auslesen von Cookies.

„Informationen": Es kommt nicht auf den Personenbezug an

Die Regelung stellt ganz allgemein auf „Informationen" ab. § 25 TTDSG ist dabei anwendbar unabhängig davon, ob der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten verarbeitet oder ob es um nicht personenbezogene Daten geht. Das hatte der Europäische Gerichtshof (EuGH) in seinem Urteil vom 01.10.2019 (Az. C-673/17 – Verbraucherzentrale Bundesverband e.V. gegen Planet49 GmbH) aufgrund einer Vorlage des Bundesgerichtshofs (BGH) bereits klargestellt.

„Endeinrichtung": Ebenfalls ein weit gefasster Begriff

Den Begriff „Endeinrichtung" definiert § 2 Abs. 2 Nr. 6 TTDSG. Die Entwurfsbegründung zum Regierungsentwurf des TTDSG (Bundestags-Drucksache 19/27441) spricht hierzu an, dass es sich damit um einen sehr weiten Anwendungsbereich handelt.

Er erfasst demnach nicht nur Telefonie oder Internetkommunikation, sei es mobil oder über das Festnetz, sondern auch die Vielzahl von Gegenständen im Internet der Dinge (IoT), die inzwischen – direkt oder über einen WLAN-Router – an das öffentliche Kommunikationsnetz angeschlossen sind. Das betrifft beispielsweise den Bereich der Smart-Home-Anwendungen, also Küchengeräte, Heizkörperthermostate, Alarmsysteme etc.

Nicht darunter fallen sollen Einrichtungen, die nicht an ein öffentliches Telekommunikationsnetz angeschlossen sind, also z.B. in einem geschlossenen Firmennetzwerk kommunizieren.

WICHTIG

Zusammengefasst: Der Anwendungsbereich von § 25 TTDSG geht weit über das hinaus, was man üblicherweise mit dem Schlagwort „Cookie-Regelung" verbindet. In der Praxis wird sich auch auswirken, dass die Regelung für diesen weiten Anwendungsbereich ab 01.12.2021 ohne Übergangsfrist gilt.

Einwilligung als Zulässigkeitsvoraussetzung

Die – personenbezogenen oder nicht personenbezogenen – Daten zu speichern bzw. auszulesen, ist „nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat" (§ 25 Abs. 1 Satz 1 TTDSG).

Der Begriff „Endnutzer" ist nicht im TTDSG definiert. Die Definition findet sich in § 3 Nr. 41 Telekommunikationsgesetz (TKG), die aufgrund der Verweisung in § 2 Abs. 1 TTDSG anwendbar ist.

Für die Anforderungen an die Einwilligung verweist § 25 Abs. 1 Satz 2 TTDSG auf die Datenschutz-Grundverordnung

(DSGVO) und damit auf Art. 4 Nr. 11, Art. 7 und Art. 8 (und soweit besondere Kategorien personenbezogener Daten betroffen sind, auf Art. 9 DSGVO).

Aus der oben erwähnten Planet49-Entscheidung des EuGH ergibt sich, dass eine aktive Einwilligung erforderlich ist. Ein voraktiviertes Häkchen genügt nicht.

Ausnahmen vom Einwilligungserfordernis

§ 25 Abs. 2 TTDSG sieht Ausnahmen vom Einwilligungserfordernis vor. Das bedeutet allerdings, dass derjenige, der sich auf die Ausnahmen beruft, ihre Voraussetzungen darlegen und beweisen können muss.

Die Art.-29-Gruppe hat sich bereits im Jahr 2012 in der „Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht" mit den Ausnahmen befasst (WP 194 vom 07.06.2012, abrufbar unter https://ogy.de/wp194). Sie hat sich dabei natürlich nicht mit § 25 TTDSG beschäftigt Doch lässt sich das Working Paper als Auslegungshilfe heranziehen. Die Ausnahme in § 25 Abs. 2 TTDSG Nr. 1 bezieht sich auf Telekommunikation, während die Nr. 2 einen weitergehenden Anwendungsbereich hat.

Ausnahmen vom Einwilligungserfordernis in der Telekommunikation

Nach § 25 Abs. 2 Nr. 1 TTDSG ist eine Einwilligung nicht erforderlich, „wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die **Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz** ist".

Der Begriff „öffentliches Telekommunikationsnetz" ist definiert als „ein Telekommunikationsnetz, das ganz oder überwiegend der Erbringung öffentlich zugänglicher Telekommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen" (§ 3 Nr. 42 TKG).

Den Begriff „Nachricht" definiert § 2 Abs. 2 Nr. 4 TTDSG als „jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen Telekommunikationsdienst ausgetauscht oder weitergeleitet wird; …".

Die Ausnahme ist damit eng begrenzt. Nach dem Wortlaut greift sie schon dann nicht mehr, wenn der Verantwortliche auch nur einen einzigen weiteren, anderen Zweck verfolgt.

Ausnahmen vom Einwilligungserfordernis bei Telemedien

Eine Einwilligung ist nach § 25 Abs. 2 Nr. 2 TTDSG des Weiteren dann nicht erforderlich, „wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen **unbedingt erforderlich** ist, **damit der Anbieter** eines Telemediendienstes **einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann**."

Was „unbedingt erforderlich" bedeutet, definiert das TTDSG nicht näher. Insbesondere diskutiert die Fachwelt, ob eine technische Erforderlichkeit bestehen muss oder ob eine wirtschaftliche Erforderlichkeit genügen kann. Sowohl § 25 TTDSG als auch Art. 5 Abs. 3 der ePrivacy-Richtlinie enthalten hierzu keine eindeutige Aussage.

Die Richtlinie 2009/136/EG, die Art. 5 Abs. 3 ePrivacy-Richtlinie geändert hat, enthält in Erwägungsgrund 66 einen Anhaltspunkt hierfür: „… sollten auf jene Situationen beschränkt sein, in denen die technische Speicherung oder der Zugriff unverzichtbar sind, um die Nutzung eines vom Teilnehmer oder Nutzer ausdrücklich angeforderten Dienstes zu ermöglichen." Diese Aussage spricht für eine technische Erforderlichkeit.

Die Art.-29-Gruppe fasst das in ihrer Stellungnahme recht griffig so zusammen: „Wenn Cookies deaktiviert sind, funktioniert der Dienst nicht." Das Erfordernis „ausdrücklich gewünscht" umschreibt die Art.-29-Gruppe so: „Der Nutzer (oder Teilnehmer) hat selbst etwas unternommen, um einen Dienst mit einem klar definierten Umfang anzufordern." Diese Auslegungen der Art.-29-Gruppe muss man nicht zwingend teilen, und erst der EuGH wird das letztverbindlich entscheiden. Teilt man die Ansicht, ist dies jedoch eine griffige Umschreibung.

Dem Wortlaut nach gilt diese Ausnahme nur für Telemediendienste. Im Bereich des „Internet der Dinge" würde diese Ausnahme also nicht gelten. Hierzu ist daher zu beachten, dass Art. 5 Abs. 3 der ePrivacy-Richtlinie eben nicht von „Telemedien" spricht, sodass es sich im Wege einer richtlinienkonformen Auslegung von § 25 Abs. 2 Nr. 2 TTDSG vermeiden lässt, die Ausnahme auf „Telemedien" zu beschränken. Hierzu beginnt aber die Diskussion jetzt erst richtig. Behalten Sie daher die weitere Auslegung im Auge!

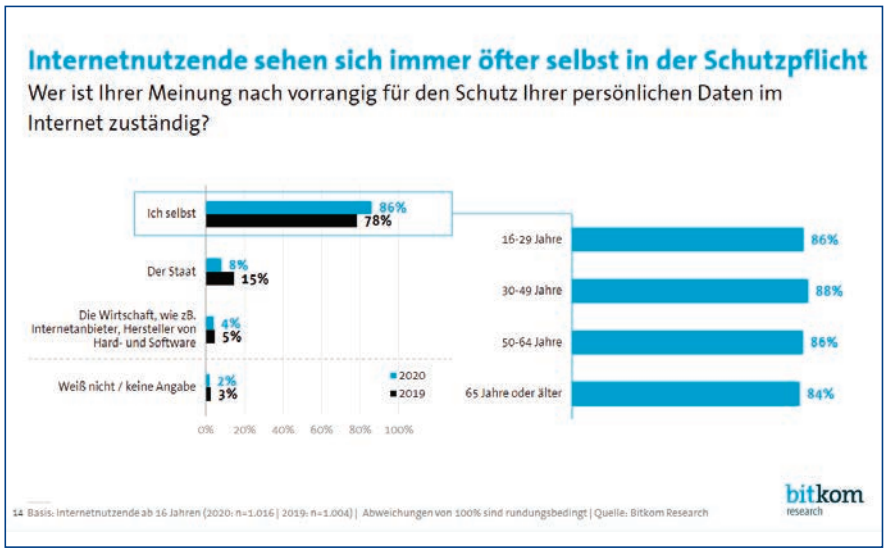
ACHTUNG!

§ 25 TTDSG setzt keine Verarbeitung personenbezogener Daten voraus. Die Zulässigkeit der Verarbeitung personenbezogener Daten im Zusammenhang mit den Vorgängen, die § 25 TTDSG regelt, richtet sich nach der DSGVO oder – sofern einschlägig – den Datenschutzbestimmungen für Telekommunikation in Teil 2 des TTDSG.

Fazit: Klare Verschärfung

Der Anwendungsbereich geht über das hinaus, was Verantwortliche üblicherweise mit dem Schlagwort „Cookie-Regelung" verbinden, und die Ausnahmen vom Einwilligungserfordernis sind recht eng begrenzt. Für Online-Tracking-Technologien ergeben sich damit auch in Deutschland klare gesetzliche Verschärfungen.

Dr. Jens Eckhardt ist Rechtsanwalt und Fachanwalt für IT-Recht, Datenschutz-Auditor (TÜV) und Compliance Officer (TÜV) bei Derra, Meyer & Partner Rechtsanwälte in Düsseldorf.



Grafik: Bitkom

Die meisten Nutzer sehen sich selbst in der Verantwortung für die Sicherheit ihrer Daten. Tools zur Selbstkontrolle über die Nutzerdaten können dabei helfen.

Datenschutz-Software

Selbstkontrolle über Nutzerdaten

Können Betroffene ihre Daten selbst kontrollieren, ist nicht nur ein wesentliches Ziel des Datenschutzes erreicht. Es hilft auch der Wirtschaft, das Vertrauen in die Digitalisierung zu steigern. Verschiedene Lösungen bieten sich für die Selbstkontrolle über Nutzerdaten an.

Das digitale Vertrauen von Kunden, Partnern und der öffentlichen Meinung zu gewinnen und zu erhalten, ist heute für den Geschäftserfolg von entscheidender Bedeutung, so das Marktforschungshaus IDC.

Befragt man aber die Kundenseite und damit Betroffene der Verarbeitung personenbezogener Daten, sieht es mit dem digitalen Vertrauen nicht so gut aus: Nur drei von zehn Internetnutzern (29 %) finden, dass ihre persönlichen Daten im Internet sicher sind, wie eine Umfrage des Digitalverbands Bitkom zeigt (siehe https://ogy.de/bitkom-vertrauen). Unter den Diensteanbietern im Internet genießen Online-Händler und E-Mail-Anbieter das meiste Vertrauen. Jeder zweite Internetnutzer (53 bzw. 50 %) vertraut ihnen jeweils stark bzw. sehr stark. Knapp dahinter liegen neue Zahlungsdienstleister sowie traditionelle Banken. 47 % sprechen ihnen jeweils das Vertrauen aus.

Viele Nutzer vertrauen sich lieber selbst

Es bleibt für fast alle Branchen festzuhalten, dass nur eine knappe Mehrheit oder sogar die Minderheit den Unternehmen bei der Datenverarbeitung vertraut.

Da mag es nicht verwundern, dass die Nutzerinnen und Nutzer sich selbst immer stärker für ihre Daten verantwortlich fühlen. Fast neun von zehn (86 %) sagen: Ich bin selbst für den Schutz meiner persönlichen Daten im Internet verantwortlich. Im Jahr 2019 waren es 78 % und 2014 erst 62 %, so Bitkom.

Das legt den Schluss nahe: Ist Vertrauen so entscheidend für den digitalen Erfolg und möchten die Nutzerinnen und Nutzer am liebsten selbst für ihre Datensicherheit sorgen, dann ist die Lösung, ihnen die Kontrolle über ihre Daten zu geben, der richtige Weg für die digitale Wirtschaft.

Wirtschaft bietet zunehmend Tools zur Selbstkontrolle

Lösungen, mit denen Online-Nutzerinnen und -Nutzer ihre personenbezogenen Daten verwalten und gezielt freigeben können, sind an sich nicht neu. In der Vergangenheit hat es hierfür schon mehrere Anläufe gegeben. Doch Marktforscher wie Gartner sind sich sicher, dass eine dezentrale Verwaltung digitaler Identitäten und personenbezogener Daten zum Standard wird (siehe https://ogy.de/5-key-predictions).

Bis 2024 soll ein echter globaler, dezentraler Identitätsstandard auf dem Markt entstehen, der geschäftliche, persönliche, soziale und gesellschaftliche Anwendungsfälle abdeckt. Damit verbunden ist, dass die Nutzer die Datenhoheit haben und selbst Anfragen für Datenzugriffe prüfen. Dabei erhält der Anfragende nur die absolut erforderliche Mindestmenge an Informationen.

Für den Datenschutz wäre dies ein idealer Zustand. Die Prognose klingt aber noch zu schön, um wahr zu werden:

- Die betroffenen Personen brauchen dafür zum einen die Sensibilisierung, wem sie wann welche Daten zu welchem Zweck und für welchen Zeitraum geben sollten.
- Zum anderen benötigen sie Werkzeuge, die die Datenhaltung und -freigabe sicher und zuverlässig bewerkstelligen. Dazu gehört v.a, dass die Nutzer damit fehlerfrei umgehen können.

Bietet die Wirtschaft Tools zur Selbstkontrolle der Nutzerdaten an, müssen diese

Werkzeuge also besonders nutzerfreundlich und leicht zu bedienen sein. Sicherheit allein genügt nicht.

Beispiel: PingOne for Individuals

PingOne for Individuals (https://ogy.de/pingone) ist ein Tool für die Selbstkontrolle. Firmen sollen damit ihren Kunden die Kontrolle über die Speicherung und Weitergabe von verifizierten personenbezogenen Daten übertragen können.

Mittels einer Digital Wallet, einer digitalen Brieftasche auf dem Mobilgerät, sollen die Nutzerinnen und Nutzer persönliche Daten verifizieren, stets aktuell speichern und unkompliziert teilen können, geschäftlich ebenso wie privat. Auch die Weitergabe von Lebensläufen, Zeugnissen, Gesundheitsakten oder anderen identitätsbezogenen Daten unterstützt das Tool, so der Anbieter.

Alle Stellen, an denen Daten zur persönlichen Identität entstehen, wie Banken oder Apotheken, können PingOne for Individuals nutzen. Sie fügen die Anmeldedaten eines Benutzers per Link oder QR-Code zu seiner digitalen Brieftasche hinzu. Andere Unternehmen oder Privatpersonen können eine Bestätigung über die Identität des Users oder Informationen zu ihm anfordern, indem sie ihn einen QR-Code auf ihrer Website, im digitalen Wallet auf ihrem Telefon oder auch auf einem ausgedruckten Stück Papier scannen lassen.

Daten ausschließlich in der digitalen Brieftasche

Sensible Daten befinden sich laut Anbieter zu keinem Zeitpunkt außerhalb der Kontrolle ihres Eigentümers, da sie ausschließlich in dessen digitalem Wallet gespeichert sind. Diese Brieftasche wird durch Blockchain-Technologie (genauer die Distributed-Ledger-Technologie von Hedera) geschützt. So lassen sich die Informationen weder verändern noch löschen Bei PingOne for Individuals liegen die personenbezogenen Daten nicht beim Unternehmen, sondern sie sind auf dem Mobilgerät des Kunden gespeichert, so der Anbieter Ping Identity.

Verbraucher können das kostenlose ShoCard Wallet direkt über den App-Store auf ihre iOS- und Android-Geräte herunterladen. Unternehmen können das PingOne for Individuals SDK (Software Development Kit) herunterladen.

Bedienbarkeit, Sicherheit und Integrierbarkeit sind Trumpf

Auf dem Markt gibt es neben diesem Anbieter bereits viele weitere Werkzeuge, die Nutzerinnen und Nutzern die Kontrolle über die eigenen Daten ermöglichen wollen. Oft sind sie als digitale Brieftasche (Wallet) organisiert und arbeiten als App auf dem Smartphone, so wie im Beispiel gezeigt.

Datenkontrolle setzt aber eine einfache Bedienbarkeit, eine hohe Sicherheit und eine breite Verwendbarkeit und damit Integrierbarkeit in Online-Plattformen voraus. Nutzer werden komplizierte Lösungen, Insellösungen und unsichere Lösungen zu Recht nicht akzeptieren.

Weisen Sie als Datenschutzbeauftragte(r) unbedingt darauf hin: Bevor ein Unternehmen seinen Kundinnen und Kunden eine solche Wallet anbietet, muss es Sicherheit, Bedienbarkeit, Integrierbarkeit und das Datenschutzniveau hinterfragen. Wünschenswert ist deshalb in Zukunft ein Datenschutz-Zertifikat nach DSGVO, aber auch eine nachprüfbare Nutzerzufriedenheit durch vertrauenswürdige Ratings in den App-Stores.

Ist dies gegeben, können Ansätze zur Selbstkontrolle bei Nutzerdaten (endlich) von Erfolg gekrönt sein. Es lohnt sich, Werkzeuge wie PingOne for Individuals entsprechend im Blick zu behalten.

Oliver Schonschek, Dipl.-Phys., ist Technology Analyst mit Fokus auf IT-Sicherheit und Datenschutz. Er wurde 2021 als „Top 25 Global Thought Leader and Influencer on Privacy" ausgezeichnet. Zudem wurde er in die Jury für die Kategorie Security beim eco award 2021 aufgenommen.

IMPRESSUM

Verlag:
WEKA MEDIA GmbH & Co. KG
Römerstraße 4, 86438 Kissing
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
Website: www.weka.de

Herausgeber:
WEKA MEDIA GmbH & Co. KG
Gesellschafter der WEKA MEDIA GmbH & Co. KG sind als Kommanditistin:
WEKA Business Information GmbH & Co. KG und als Komplementärin:
WEKA MEDIA Beteiligungs-GmbH

Geschäftsführer:
Stephan Behrens, Michael Bruns, Jochen Hortschansky, Kurt Skupin

Redaktion:
Ricarda Veidt, M.A. (V.i.S.d.P)
E-Mail: ricarda.veidt@weka.de

Anzeigen:
Anton Sigllechner
Telefon: 0 82 33.23-72 68
Fax: 082 33.23-5 72 68
E-Mail: anton.sigllechner@weka.de

Erscheinungsweise:
Zwölfmal pro Jahr

Aboverwaltung:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-740
E-Mail: service@weka.de

Abonnementpreis:
12 Ausgaben 232,00 €
(zzgl. MwSt. und Versandkosten)
Einzelheft 22 €
(zzgl. MwSt. und Versandkosten)

Druck:
Geiselmann Printkommunikation GmbH
Leonhardstraße 23, 88471 Laupheim

Layout & Satz:
METAMEDIEN
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4095

ISSN-Nr.:
1614-6867

Bestellung unter:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
www.datenschutz-praxis.de

Haftung:
Die WEKA MEDIA GmbH & Co. KG ist bemüht, ihre Produkte jeweils nach neuesten Erkenntnissen zu erstellen. Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert.
Bei Nichtlieferung durch höhere Gewalt, Streik oder Aussperrung besteht kein Anspruch auf Ersatz. Erfüllungsort und Gerichtsstand ist Kissing. Zum Abdruck angenommene Beiträge und Abbildungen gehen im Rahmen der gesetzlichen Bestimmungen in das Veröffentlichungs- und Verbreitungsrecht des Verlags über. Für unaufgefordert eingesandte Beiträge übernehmen Verlag und Redaktion keine Gewähr. Namentlich ausgewiesene Beiträge liegen in der Verantwortlichkeit des Autors bzw. der Autorin.

Datenpannen

Data Breach Nikolaus

Kinder und Jugendliche rechtzeitig mit dem Thema „Datenschutz“ vertraut zu machen, ist mehr als sinnvoll. Doch das kann manchmal auch ungeahnte Folgen haben.

Als Datenschutzbeauftragter nehme ich mit Vergnügen Einladungen von Klassenlehrerinnen und Klassenlehrern an, die mich bitten, in ihren Klassen über das Thema „Datenschutz“ im Zusammenhang mit Social Media und Messengern zu sprechen.

Besonders gern mache ich das in der fünften Klassenstufe. Das sind Schülerinnen und Schüler, die gerade auf eine weiterführende Schule gekommen sind. Und das ist normalerweise auch der Zeitpunkt, zu dem die Eltern ihnen ein Smartphone zur Verfügung stellen. Und damit wird die Frage nach dem Verhalten im Bereich Social Media und Messenger akut.

Zu intensives Training?

Dass ich das wohl in einem Fall etwas zu intensiv trainiert hatte, zeigt folgende Geschichte: Ein Vater rief mich kurz nach Nikolaus an, um mir eine Begebenheit zu erzählen, die ihn sehr zum Lachen gebracht hatte. Sein Sohn war nämlich – wie der Vater selbst auch – bei der Projektveranstaltung in der Schule dabei. Er ist das älteste von drei Kindern. Das jüngste, ein Mädchen, ist vier Jahre alt.

Kritik vom Nikolaus

Am 6. Dezember nun wurde der Onkel der beiden, verkleidet als Nikolaus, zum gerechten Vorbild, das eine erzieherische Wirkung auslösen sollte. Neben vielen positiven Eigenschaften erwähnte der Nikolaus auch ein paar Kritikpunkte. Das kleine Mädchen war sehr geknickt: Vieles von dem, was der vermeintliche Nikolaus sagte, musste genau getroffen haben. Der elfjährige Bruder sah das und sprang seiner Schwester bei.

Der Bruder eilt zu Hilfe

„Da sind soeben personenbezogene Daten von hoher Schutzstufe unbefugt preisgegeben worden. Der Nikolaus hat nicht das Recht, personenbezogene Daten, die nur die Schwester betreffen, in aller Öffentlichkeit auszubreiten. Das ist ein Verstoß gegen den Datenschutz, das haben wir erst vor ein paar Tagen in der Schule gelernt. Eigentlich wäre das sogar meldepflichtig bei der Aufsichtsbehörde!“

Nach einer kurzen Pause des Erschreckens lachte die ganze Gesellschaft aus vollem Hals. Volltreffer. Datenschutz in perfekter Anwendung.

Eberhard Häcker ist seit vielen Jahren externer Datenschutzbeauftragter. Als ehemaliger Berufsschullehrer gibt er sein Wissen auch gern in Schulen weiter.

IN DER NÄCHSTEN AUSGABE

10 Regeln für Social Media

Beim Marketing beliebt, bei DSB weniger – lassen sich Risiken, die mit Social Media verbunden sind, in den Griff bekommen?

Was tun gegen Innentäter?

Bonusjäger, Vernachlässigte und Zurückgesetzte – das sind nur einige Typen bewusst handelnder Innentäter von vielen.

Daten als Gegenleistung

Die Digitale-Inhalte-Richtlinie, national umgesetzt im BGB, mischt die Karten neu in Bezug auf das Kopplungsverbot.