www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT | Mai 2021

Bild: iStock.com/muhamad rukmana

Beim Schadenersatz geht es zwar bisher nicht um Millionensummen. Doch die Wahrscheinlichkeit, vor Gericht mit Schadenersatz konfrontiert zu sein, ist wesentlich höher, als ein Bußgeldverfahren zu erleben.

Haftungsrisiken

Schadenersatz nach DSGVO: Das zeigen die aktuellen Urteile

Jeden Monat gibt es derzeit neue Entscheidungen deutscher Gerichte zum Schadenersatz. Und sie fallen immer häufiger zugunsten der betroffenen Person aus. Wie verteidigen sich Verantwortliche gegen Schadenersatzansprüche, welche Fallstricke gilt es zu vermeiden?

Bußgelder waren lange das Thema Nummer eins. Doch bisher gab es in Deutschland nur wenige Verfahren, in denen es um Bußgelder in Millionenhöhe ging. Ganz anders verhält es sich bei den Schadenersatzansprüchen nach Art. 82 Datenschutz-Grundverordnung (DSGVO).

Die DSGVO regelt nicht nur die klassischen Betroffenenrechte wie Recht auf Auskunft, Löschung oder Widerspruch. Die betroffene Person hat darüber hinaus unterschiedliche Möglichkeiten, diese Rechte geltend zu machen oder sich gegen DSGVO-Verstöße durch den Verantwortlichen zu wehren.

Schadenersatz nach Art. 82 DSGVO

Dazu gehört zum einen das Beschwerderecht bei den Datenschutzaufsichtsbehörden. Zum anderen regelt die DSGVO, dass jeder einen Anspruch auf Schadenersatz gegen den Verantwortlichen oder den Auftragsverarbeiter hat, wenn ihm durch die Verarbeitung ein Schaden entstanden ist. Jede Person hat einen Schadenersatzanspruch

1. bei einem Verstoß gegen die DSGVO,
2. wenn sie einen Schaden erlitten hat,
3. dieser Schaden auf dem Verstoß beruht und
4. der Verantwortliche oder Auftragsverarbeiter schuldhaft gehandelt hat.

Fehlt es auch nur an einer dieser Voraussetzungen, besteht kein Schadenersatzanspruch, und die betroffene Person geht leer aus. Was hat es aber mit diesen vier Punkten genau auf sich?

1. Verstoß gegen die DSGVO

Für einen Verstoß nach Art. 82 DSGVO genügt jede Verletzung datenschutz- →

Editorial

Ricarda Veidt,
Chefredakteurin

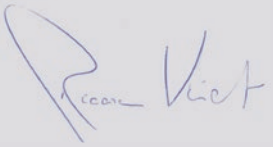
Der böse Datenschutz

Liebe Leserin, lieber Leser! „Der Datenschutz" als Verhinderer und Bremser – das ist gerade wieder eine äußerst beliebte Sicht der Dinge. Falls Sie nicht wie ich das Vergnügen hatten, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Prof. Ulrich Kelber auf den FFD-Datenschutztagen zu hören: Er hat gründlich mit diesem Vorwurf aufgeräumt.

Keine einzige wirksame, geeignete und erforderliche Maßnahme zur Pandemie-Bekämpfung sei am Einspruch des BfDI gescheitert. Der Datenschutz sei, entgegen der Meinung in Talkshows und ähnlichen Runden, auch nicht das einzige Grundrecht, das ungeschoren davongekommen wäre. Und für die Versäumnisse in der Digitalisierung sei er ebenfalls nicht verantwortlich, selbst wenn es bequem sei, das zu behaupten.

„Faktenfreiheit scheint ein neuer Volkssport geworden zu sein", so seine auf den Punkt gebrachte Beurteilung, verbunden mit dem Aufruf an alle Datenschutzbeauftragten, dem „Narrativ vom bösen Datenschutz" mit Argumenten entgegenzuwirken, so mühsam es auch sei.

Herzliche Grüße
Ihre Ricarda Veidt



rechtlicher Vorschriften. Es muss sich nicht um eine Vorschrift handeln, die gezielt der betroffenen Person dient. Zu den Verstößen zählen demnach nicht nur die verspätete Auskunft, sondern auch fehlende Datenschutzerklärungen oder ein Verstoß gegen die rechtmäßige Verarbeitung gemäß Art. 6 DSGVO.

Umfasst sind auch formelle Verstöße des Verantwortlichen, etwa wenn

- er keinen Datenschutzbeauftragten bzw. keine Datenschutzbeauftragte bestellt hat, obwohl er dazu verpflichtet ist,
- er das Verzeichnis der Verarbeitungstätigkeiten nicht oder fehlerhaft führt oder
- kein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO vorliegt.

Ob es sich um einen geringfügigen oder um einen gravierenden Verstoß gegen die DSGVO handelt, spielt keine Rolle.

2. Schaden

Weiterhin muss die Person aufgrund dieses Verstoßes einen Schaden erlitten haben. Ein Schaden kann materieller oder immaterieller Art sein. Unter materielle Schäden fallen wirtschaftliche Nachteile wie Kreditkartenbetrug oder Identitätsdiebstahl. Denkbar sind auch körperliche Schäden, beispielsweise wenn ein Krankenhaus Angriffsziel einer Cyberattacke wird, es medizinische Geräte dadurch nicht mehr nutzen und deswegen Patienten nicht behandeln kann.

Weitaus häufiger haben sich die deutschen Gerichte bisher mit dem immateriellen Schaden befasst. Unter immaterielle Schäden fallen beispielsweise Diskriminierung, Rufschädigung oder der Verlust von Rechten. Typische Beispiele sind

- die unbefugte Veröffentlichung von Fotos oder schützenswerten Informationen im Internet,
- unbefugte Übermittlung von Gesundheitsdaten an Dritte,
- Weiterleitung von privaten Nachrichten oder
- verspätete Beantwortung eines Auskunftsersuchens.

An dieser Stelle wird es besonders brisant: Bisher waren die deutschen Gerichte äußerst zurückhaltend, wenn es um immaterielle Schäden ging. Sie waren der Meinung, dass unbedeutende oder nur geringfügige Schäden nicht zu ersetzen sind. Schadenersatz gab es nur bei erheblichen und spürbaren Nachteilen. Seit einiger Zeit zeigt sich jedoch eine Trendumkehr. Einige Gerichte sind der Meinung, dass es beim Schadenersatz keine Bagatellgrenze gibt. Das heißt, dass jeder Schaden zu ersetzen ist. Daher wird es äußerst spannend, was der EuGH dazu sagen wird.

ACHTUNG!

Das letzte Wort in Sachen „immaterieller Schaden" wird der Europäische Gerichtshof (EuGH) haben. Dem EuGH wurde erst kürzlich die Frage vorgelegt, ob Art. 82 DSGVO auch immaterielle Schäden umfasst, die nur geringfügig sind. Sollte der EuGH zum Ergebnis kommen, dass geringfügige Schäden ebenfalls umfasst sind, dürfte das der Startschuss für eine neue Klagewelle sein. Betroffene Personen könnten deutlich häufiger vor den Zivil- und Arbeitsgerichten klagen.

3. Kausalität

Die betroffene Person hat nur dann einen Schadenersatzanspruch, wenn der Schaden auf einem Verstoß gegen die DSGVO beruht. Das dürfte der Regelfall sein. Hintergrund dieser Voraussetzung ist, dass der Verantwortliche keinesfalls für jeden Schaden haften soll, sondern nur für solche, die er auch verursacht hat.

Ausnahmsweise dürfte ein Schaden dem Verantwortlichen nicht zuzurechnen sein, wenn der Schaden aufgrund höherer Gewalt entstanden ist oder weil ein Dritter unbefugt gehandelt hat. Kommt es beispielsweise aufgrund eines Unwetters zu einem Blitzeinschlag im Gebäude des Verantwortlichen und wird der Server dadurch beschädigt, sodass Daten kurzfristig nicht mehr verfügbar sind, so lässt sich dies dem Verantwortlichen nicht anlasten.

Zweifelhaft, aber zulässig

Geschäftsmodell Schadenersatz

Interessant ist, dass es schon heute Geschäftsmodelle gibt, die sich mit dem Thema Schadenersatz nach DSGVO auseinandersetzen. So machen einige Unternehmen im Auftrag Schadenersatzansprüche geltend. Die betroffene Person gibt lediglich ihre Kontaktdaten an und tritt ihre Ansprüche teilweise ab. So erhalten die Unternehmen eine Erfolgsprovision von bis zu 25 % des Schadenersatzes. Dieses Geschäftsmodell hat sich bereits bei Fluggastrechten etabliert. Auch wenn dieses Geschäftsgebaren zweifelhaft ist, so hat der Verantwortliche hiergegen keinerlei Handhabe.

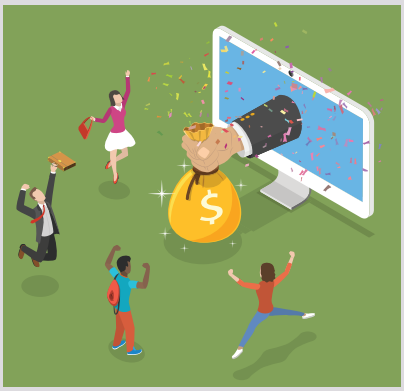


Bild: iStock.com/TarikVision

4. Verschulden

Eine betroffene Person, die vor Gericht einen Schadenersatzanspruch geltend machen will, muss grundsätzlich alle Voraussetzungen für einen Anspruch nach Art. 82 DSGVO darlegen und beweisen können.

Das ist gar nicht so einfach. Denn die betroffene Person kann häufig nur einen Schaden bei sich selbst feststellen. Wie es zu diesem Schaden kam, ob und unter welchen Umständen ein Verantwortlicher oder Auftragsverarbeiter gegen die DSGVO verstoßen hat, ist für die betroffene Person schwer zu beweisen. Sie kann sich nicht wie die Datenschutzaufsichtsbehörden Dokumente vorlegen lassen oder eine Prüfung im Unternehmen durchführen.

Dieses Dilemma zeigt sich auch in der gerichtlichen Praxis. In den Fällen, in denen Gerichte Schadenersatzansprüche abgelehnt haben, konnte der Kläger einen Verstoß des Verantwortlichen nicht beweisen. Das ist aber noch lange kein Grund für Verantwortliche, sich entspannt zurückzulehnen. Denn die DSGVO hat eine Beweislastumkehr vorgesehen. Nach Art. 82 Abs. 3 DSGVO haftet der Verantwortliche oder der Auftragsverarbeiter nicht, wenn er nachweisen kann, dass er in keinerlei Hinsicht für den entstandenen Schaden verantwortlich ist. Das bedeutet, es wird regelmäßig vermutet, dass der Schaden dem Verantwortlichen zugerechnet wird.

PRAXIS-TIPP

Wichtig zu wissen ist, dass der Verantwortliche sich nicht damit entschuldigen kann, dass nicht er, sondern sein Auftragsverarbeiter den Schaden herbeigeführt hat. Verantwortliche können sich regelmäßig nur entlasten, indem sie nachweisen, dass sie

- Mitarbeiter regelmäßig schulen,
- Datenschutzaudits durchführen und
- bei Zweifeln oder Unklarheiten die Datenschutzaufsichtsbehörden kontaktieren oder sonstige Rechtsberatung einholen.

Wer für den entstandenen Schaden zahlen muss

Sinn und Zweck von Art. 82 DSGVO ist es, die betroffene Person weitestgehend zu entschädigen. Dafür ist Voraussetzung, dass sie eine Möglichkeit hat, an den Verursacher heranzutreten.

In der Praxis sind üblicherweise mehrere Akteure an einer Verarbeitung beteiligt. Hinzu kommt, dass die an einer Verarbeitung Beteiligten nicht nur innerhalb Deutschlands, sondern in der EU bzw. im Europäischen Wirtschaftsraum (EWR) unterschiedliche Niederlassungen haben oder in einem Drittland ansässig sind.

Doch das soll kein Nachteil für die betroffene Person sein. Um sicherzustel- →

PRAXIS-TIPP

Verantwortliche und Auftragsverarbeiter sollten unbedingt vertraglich regeln, wer und unter welchen Voraussetzungen im Innenverhältnis Regress nehmen kann. Regressklauseln gehören in den Vertrag zur Auftragsverarbeitung oder in die Vereinbarung zur gemeinsamen Verantwortlichkeit. Außerdem lohnt es sich, Versicherungspolicen zu prüfen. Immer mehr Versicherer bieten gute Cyberversicherungen an, die auch Schäden bei Dritten decken. Das schützt zwar nicht vor jedem Schadenersatzanspruch, reduziert aber das Risiko für den Verantwortlichen oder den Auftragsverarbeiter erheblich.

len, dass die betroffene Person in jedem Fall den Schaden ersetzt bekommt, haftet jeder an der Verarbeitung Beteiligte, wenn er für den Schaden verantwortlich ist. „Verantwortlich" ist in diesem Kontext nicht wörtlich zu nehmen, sondern als Verursacher des Schadens zu verstehen. Es spielt keine Rolle, ob der Schadensverursacher (gemeinsam) Verantwortlicher oder Auftragsverarbeiter im Sinne der Datenschutz-Grundverordnung ist.

Für die betroffene Person hat dies den Vorteil, dass sie sich aussuchen kann, wem gegenüber sie letztlich ihren Schadenersatzanspruch geltend macht. Und die Wahl wird ihr leicht gemacht. Um das Prozessrisiko so gering wie möglich zu halten, wird sie sich an den wenden, der seinen Sitz in Deutschland hat und zahlungskräftig ist. Denn auch ein gewonnener Schadenersatzprozess nützt nichts, wenn der Gegner zahlungsunfähig ist.

Das Gerichtsverfahren

Interessant ist auch der Aspekt, dass die deutschen Aufsichtsbehörden beim Thema Schadenersatzanspruch nur eine untergeordnete Rolle spielen. Jeder, der meint, er hat aufgrund eines Verstoßes des Verantwortlichen oder Auftragsverarbeiters einen Schaden erlitten, kann vor den Zivil- und Arbeitsgerichten klagen.

Die deutschen Aufsichtsbehörden sind für Schadenersatzansprüche nach der DSGVO nicht zuständig. Die Datenschutzaufsichtsbehörden führen nur Bußgeldverfahren oder aufsichtliche Verfahren. Das sollten Verantwortliche berücksichtigen, wenn sie sich gegen Schadenersatzansprüche wehren. Es empfiehlt sich daher, neben der oder dem Datenschutzbeauftragten auch Rechtsanwälte einzubinden, die im Bereich des Zivilrechts oder Arbeitsrechts tätig sind.

Typische Fallstricke vermeiden

Zwar gibt es mittlerweile eine Vielzahl von Gerichtsentscheidungen zu Art. 82 DSGVO. Doch es zeichnet sich ab, dass es immer um die gleichen Verstöße geht. In den Gerichtsverfahren, in denen das Gericht Schadenersatz zugesprochen hat, ging es häufig um folgende Fälle:

- unbefugte Veröffentlichung privater Daten im Internet, insbesondere Fotos von Mitarbeitenden
- unbefugte Übermittlung von Gesundheitsdaten eines Arbeitnehmers oder einer Arbeitnehmerin
- keine Auskunft erteilt
- Auskunftsanfrage verspätet beantwortet

Verantwortliche können diese Fallstricke leicht vermeiden:

- Bei den Betroffenenrechten muss sichergestellt sein, dass die zuständige Abteilung die Anfragen schnellstmöglich bekommt. Nur so lässt sich die einmonatige Frist zur Beantwortung einhalten.
- Geht es um personenbezogene Daten von Mitarbeiterinnen und Mitarbeitern, sollte der Verantwortliche besonders sorgsam sein. Haben Arbeitnehmer das Unternehmen verlassen, sollten sämtliche Daten, insbesondere online veröffentlichte Daten, unverzüglich gelöscht werden. Ausnahme: Es gelten Aufbewahrungspflichten.

Keine Dokumente voreilig herausgeben

Verantwortliche sollten Drohungen im Zusammenhang mit Schadenersatzansprüchen ernst nehmen, aber nicht voreilig handeln. Auf keinen Fall sollten Verantwortliche interne Dokumente ohne Rücksprache mit einem Rechtsanwalt herausgeben. Das gilt v.a. für das Verzeichnis gemäß Art. 30 DSGVO, die Datenschutz-Folgenabschätzung oder Verträge nach Art. 26 und 28 DSGVO.

Hierbei handelt es sich um Dokumente, die auch Geschäftsgeheimnisse enthalten und nur für den Verantwortlichen und die Datenschutzaufsichtsbehörden bestimmt sind. Nur dann, wenn es im Prozess dienlich ist und den Verantwortlichen entlasten kann, sollten er diese Dokumente im Prozess vorlegen.

Fazit: Schadenersatzrisiko nicht einfach ausblenden!

Ein Blick auf die Gerichtsverfahren zeigt, dass das Risiko eines Schadenersatzprozesses höher ist als das eines Bußgeldverfahrens. Verantwortliche sollten diese Entwicklung zum Anlass nehmen, um im nächsten Datenschutzaudit typische Fallstricke zu prüfen. Dazu gehört v.a. der Umgang mit Betroffenenanfragen.

Wer sich bei der Beantwortung zu viel Zeit lässt, gar nicht erst antwortet oder Auskunftsersuchen nur mangelhaft erfüllt, riskiert einen Schadenersatzprozess.

Besonderes Augenmerk sollten Verantwortliche daneben auf den Beschäftigtendatenschutz legen. Vor allem Arbeitsgerichte neigen dazu, die Voraussetzungen von Art. 82 DSGVO sehr wohlwollend auszulegen. Im Fall eines Gerichtsverfahrens stehen die Chancen für den Arbeitnehmer oder die Arbeitnehmerin besonders gut.

Weitgehende Einigkeit bei der Höhe des Schadenersatzes

Übrigens sind sich die Gerichte ausnahmsweise in einem Punkt einig: Bei einem Verstoß gegen Betroffenenrechte werden zwischen 1.000 € und 5.000 € fällig. Obendrauf kommen die Gerichtskosten sowie die Gebühren für den eigenen und den gegnerischen Anwalt.

PRAXIS-TIPP

Und noch eines zeigen die Gerichtsentscheidungen: Wer bei den Betroffenenanfragen sorgfältig arbeitet, seine Dokumentation gewissenhaft führt und sie aktuell hält, der macht nicht nur bei einer Prüfung der Datenschutzaufsichtsbehörden eine gute Figur. Auch gegen Schadenersatzansprüche kann er sich erfolgreich verteidigen.

Kristin Benedikt ist seit April 2020 Richterin am Verwaltungsgericht Regensburg. Zuvor leitete sie von 2015 bis 2020 den Bereich Internet beim Bayerischen Landesamt für Datenschutzaufsicht.

Bild: iStock.com/AndreyPopov

Welche Empfehlungen der EDSA gibt, um Datenpannen im Vorfeld zu vermeiden, lesen Sie in der nächsten Ausgabe im zweiten Teil

Praktische Fallbeispiele

Leitlinien des EDSA: Mit Datenpannen richtig umgehen

Wie erkennen Mitarbeitende Datenpannen? Wie sorgen wir dafür, dass sie sie auch rechtzeitig melden? Das sind in der Praxis immer wieder schwierige Themen. Unterstützung für die Schulung bieten aktuelle Leitlinien des Europäischen Datenschutzausschusses (EDSA).

Zu den Aufgaben des EDSA gehört es u.a., Leitlinien bereitzustellen, um eine einheitliche Anwendung der Datenschutz-Grundverordnung (DSGVO) sicherzustellen. Die „Guidelines 01/2021 on Examples regarding Data Breach Notification" vom Januar 2021 schreiben bisherige Leitlinien der Artikel-29-Gruppe fort und ergänzen sie. Leider ist der vollständige Text bisher nur in englischer Sprache verfügbar unter https://ogy.de/guidelines-examples-data-breach.

Aufbau der Leitlinien

Die Leitlinien orientieren sich an neueren Einzelfallbeispielen aus den Erfahrungen der Aufsichtsbehörden. Der EDSA teilt die Datenpannen in sechs Kategorien ein:

- Ransomware
- Angriffe mit Datenverlusten
- Mitarbeiterfehler bzw. -fehlverhalten
- verlorene/gestohlene Geräte bzw. Papierdokumente
- Fehlversand von Post bzw. E-Mail
- Social Engineering

Datenpannen erkennen und Gegenmaßnahmen einleiten

Diese Datenpannen-Kategorien erläutert die Leitlinie anschaulich mit konkreten Fallbeispielen. Zu jedem Fallbeispiel gibt der EDSA Hinweise, wie sich eine solche Datenpanne im Vorfeld hätte verhindern lassen. Außerdem führen die Leitlinien auf, was Verantwortliche im konkreten Einzelfall tun müssen, um ihren Verpflichtungen nach Art. 33 und 34 DSGVO nachzukommen und wie sie Schadensrisiken für die betroffenen Personen minimieren.

Zu jedem Einzelfall legen die Leitlinien dar, ob eine Meldung an die Aufsichtsbehörde und eine Information der betroffenen Personen notwendig sind.

Zu jeder Kategorie von Datenpannen enthalten die Leitlinien konkrete Handlungsanweisungen zu technisch-organisatorischen Maßnahmen, um derartige Datenpannen zu verhindern, sowie Vorschläge, um den Schaden zu begrenzen.

Dokumentation ist zwingend

Alle Datenpannen gehören in die interne Dokumentation des Unternehmens. Das sieht Art. 33 Abs. 5 DSGVO vor. Diese Dokumentation ist unabhängig davon, ob es sich gegenüber der Aufsichtsbehörde um eine meldepflichtige Datenpanne handelt oder ob die Meldung nicht nötig ist, und ob die betroffenen Personen über die Datenpanne zu informieren sind. →

ACHTUNG!

Die Leitlinien betonen, dass es sich um konkrete Einzelfallbeispiele handelt. Bei geänderten Tatsachen können also andere oder intensivere Maßnahmen als die genannten notwendig sein. Damit geben die Leitlinien Anhaltspunkte für Maßnahmen. Aber nicht mehr! Verantwortliche müssen also immer bei einer Datenpanne ganz genau prüfen, welche Panne vorliegt, wo Risiken liegen, wie hoch diese für die betroffenen Personen sind und was konkret zu tun ist.

Andrea Gailus ist Rechtsanwältin mit Schwerpunkt Datenschutzrecht. Außerdem ist sie Autorin des E-Learning „Grundlagen des Datenschutzes".

Fallbeispiel mit Details	Meldung Aufsicht	Information Betroffene
Kategorie der Datenpanne: Ransomware		
Daten verschlüsselt, elektronisches separates Backup vorhanden, durch Angriff nur Zugriff auf Daten gesperrt und kein Datenverlust, Wiederherstellung des Datenzugriffs durch Backup innerhalb einiger Stunden, wenige personenbezogene Daten betroffen	nein	nein
Daten unverschlüsselt, kein elektronisches Backup vorhanden, nur in Papierform, durch Angriff nur Zugriff auf Daten gesperrt und kein Datenverlust, Wiederherstellung des Datenzugriffs durch Papier-Backup dauert fünf Tage, es entstehen Lieferverzögerungen, Daten von Mitarbeitern und Kunden betroffen	ja	nein
Daten eines Krankenhauses nicht verschlüsselt, elektronisches Backup vorhanden, Angriff sperrt Zugriff auf Daten ohne Datenverlust, Wiederherstellung dauert zwei Tage, Daten von Mitarbeitern und Patienten betroffen, durch Nichtverfügbarkeit müssen Operationen verschoben oder abgesagt werden	ja	ja
Daten nicht verschlüsselt, Backup vorhanden, aber nicht separat aufbewahrt, Angriff verschlüsselt Daten und führt zu Datenverlust, Backup ebenfalls verschlüsselt und nicht mehr zugänglich, betroffen sind personenbezogene Daten und Kreditkartennummern	ja	ja
Kategorie der Datenpanne: Angriff mit Datenverlust		
Cyberattacke mit Einbringen eines Schadcodes und Datenverlust (Bewerberdaten)	ja	ja
Datenverlust von (per Hashwert gesicherten) Passwörtern einer Website, 1.200 Nutzer betroffen, nur Pseudonyme als Nutzername zulässig	nein	nein
Cyberattacke auf Online-Banking-Website, Name, Geburtsdatum, Steuernummer von 100.000 Betroffenen offengelegt, Einloggen des Angreifers in 2.000 Konten möglich, doch keine Zahlungstransaktionen	ja	ja
Kategorie der Datenpanne: Mitarbeiter		
ehemaliger Mitarbeiter hat Kontaktdaten von Kunden für eigene Geschäftstätigkeit genutzt	ja	nein
versehentliche Übermittlung von Daten an Versicherungsvertreter, Kontakt- und Versicherungsdaten betroffen, Vertreter meldet dies selbst, löscht nach Aufforderung alles und bestätigt die Löschung	nein	nein
Kategorie der Datenpanne: Diebstahl/Verlust von Geräten oder Dokumenten		
Diebstahl von Tablets (passwortgeschützt) mit verschlüsselten personenbezogenen Daten, Backup vorhanden, Remote-Zugang ermöglicht Löschen der Daten auf gestohlenen Geräten	nein	nein
Diebstahl Notebook ohne Passwort & Verschlüsselung, 100.000 Kunden betroffen, Name, Geschlecht, Geburtstag, Adressen zugänglich, unklar, ob weitere Datenkategorien betroffen, Wiederherstellung per Backup	ja	ja
Papierdokumente mit Gesundheitsdaten werden gestohlen, Dokumente waren nicht in Schrank verschlossen, Raum nicht verschlossen, keine Zugangs-/Zugriffskontrollen geregelt, kein Backup vorhanden	ja	ja
Kategorie der Datenpanne: Fehlversand		
Fehlversand von zwei Produkten mit verwechselten Rechnungen, Rückruf, Versand an korrekte Empfänger	nein	nein
Fehlversand infolge eines Maschinenfehlers, ein Umschlag enthält zwei Briefe	ja	nein
Liste mit Bewerberdaten wird versehentlich an eine E-Mail angehängt, betroffen sind Daten von 60.000 Personen, Empfänger der E-Mail werden gebeten, den Anhang der E-Mail zu löschen	ja	ja
E-Mail-Fehlversand für einen Sprachkurs, betroffene Daten: Namen, E-Mail-Adressen, Hinweise auf Lactose-Intoleranz von zwei Teilnehmenden, sofortige Bitte um Löschung der E-Mail	nein	nein
Kategorie der Datenpanne: Social Engineering		
Identitätsdiebstahl: Daten einer Person betroffen, E-Mail-Adresse zum Rechnungsempfang wurde auf telefonische Bitte geändert, Fragen zur Identifikation des Anrufers gemäß Unternehmensrichtlinie gestellt	ja	ja
Social-Engineering-Angriff führt dazu, dass bestimmte E-Mails des Unternehmens an eine externe Adresse weitergeleitet werden, betroffen sind Daten von 99 Mitarbeitern	ja	ja

Überblick über Beispiele von Datenpannen und die damit verbundenen Meldepflichten entsprechend der EDSA-Leitlinie

Bild: BMI/Bundesdruckerei

Betroffenenrechte und Sicherheit der Identitäten

Identifizierung bei Auskunftsersuchen

Wie lässt sich die Identität einer Auskunft suchenden betroffenen Person überprüfen, insbesondere im Rahmen von Online-Diensten? Kann die Online-Ausweisfunktion des Personalausweises helfen? Wie sind andere digitale Identitätsdienste zu beurteilen, wenn sie ein Betroffener oder eine Betroffene als Nachweis nutzen möchte?

Die Betroffenenrechte nach Datenschutz-Grundverordnung (DSGVO) zu erfüllen, bereitet weiterhin Probleme. Geht z.B. ein Antrag auf Auskunft ein und der Verantwortliche erteilt die Auskunft fristgerecht, doch der Antragsteller war gar nicht die betroffene Person, sind personenbezogene Daten in falsche Hände gelangt.

Deshalb ist es ein wichtiger Teil der Umsetzung des Auskunftsrechts, die Identität des Antragstellers oder der Antragstellerin zu überprüfen (Erwägungsgrund 64 DSGVO). Gefälschte digitale Identitäten sind leider keine Seltenheit. So basieren die um sich greifenden Phishing-Attacken auf einer gefälschten digitalen Identität, die vertrauliche Daten herauslocken soll.

Identifizierung über digitale Verfahren

In Zeiten der fortschreitenden Digitalisierung sind teilweise geschwärzte Kopien des Personalausweises, per Post verschickt, für manche betroffenen Personen nicht mehr der Weg der Wahl.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) Baden-Württemberg hatte bereits 2019 auf digitale Alternativen wie die Identifizierung über ein Nutzerkonto, Video-Ident-Identifizierung und die Identifizierung über einen eIDAS-Dienst (electronic IDentification, Authentication and trust Services) hingewiesen (siehe https://ogy.de/ldfi-bw-identitaetspruefung). Allerdings gab es 2019 bei diesen digitalen Alternativen einige Punkte zu beachten:

- Dienste nach der eIDAS-Verordnung haben Bürgerinnen und Bürger noch nicht in größerem Umfang genutzt.
- Aus Datenschutzsicht weniger schön ist, dass eine Schwärzung der Videoaufnahme des Ausweisdokuments nicht ohne Weiteres möglich ist. Fraglich war deshalb, ob datenschutzbewusste Bürger bereit sind, eine Video-Ident-Identifizierung durchzuführen.
- Die Sicherheit des Identifizierungsverfahrens über ein Nutzerkonto hängt stark vom Passwort ab. Können Angreifer Nutzerkonten übernehmen, lassen sich damit weitere Daten ausspähen, womöglich dann über ein Auskunftsersuchen mit gefälschter Identität.

Nun stellt sich die Frage, ob die digitalen Verfahren bei der Identifizierung →

Immer noch eine Möglichkeit

Der Klassiker: die Ausweiskopie

Eine Recherche im Internet liefert Beispiele, wie Unternehmen und Behörden die Verfahren für ein Auskunftsersuchen umsetzen und die Identität des Antragstellenden überprüfen. Wer etwa ein Auskunftsersuchen zu gespeicherten Fluggastdaten an das Bundeskriminalamt richtet, soll bei einem postalischen Antrag eine gut leserliche Kopie eines aktuellen Ausweisdokuments beifügen (siehe https://ogy.de/auskunft-bka). Eine wichtige Empfehlung: Die Aufsichtsbehörden für den Datenschutz haben darauf hingewiesen, dass man als betroffene Person die nicht erforderlichen persönlichen Daten auf der Kopie des Ausweises (wie Augenfarbe, Größe, ID-Nummer, Unterschrift) schwärzen sollte.

von Auskunftsersuchenden inzwischen besser helfen. Dazu seien einige Verfahren der digitalen Identitätsprüfung näher betrachtet.

De-Mail

Zum Auskunftsrecht schreibt der Bundesdatenschutzbeauftragte: „Es empfiehlt sich daher, die Auskunft schriftlich oder in einer sicheren elektronischen Form (z.B. per De-Mail oder mittels verschlüsselter E-Mail über das Programm Pretty Good Privacy (PGP) oder GnuPG) anzufordern."

Doch wie steht es um die Verbreitung von De-Mail, gerade auch bei Privatpersonen, die sich als Auskunftsersuchende an Unternehmen wenden? In einem Bericht stellte der Bundesrechnungshof fest: „Allerdings kann der Bundesrechnungshof nicht erkennen, dass sich De-Mail bislang als Standardverfahren für rechtssichere elektronische Kommunikation etabliert hat. Dies bestätigen insbesondere der niedrige Nutzungsgrad und die geringe Akzeptanz von De-Mail." Offensichtlich kann ein Unternehmen also nicht davon ausgehen, mit De-Mail viele Identitäten bei Auskunftsersuchen klären zu können.

Identifizierung über Nutzerkonten

Es gibt zwar inzwischen eine Vielzahl an Online-ID-Diensten und Identity-Providern im Internet. Doch ein Identitätsnachweis über einen solchen Identity-Provider hängt grundsätzlich von der Sicherheit, von der Vertrauenswürdigkeit und von der Verbreitung der Online-ID ab.

- So stellt sich die Frage, wie der Anbieter die Identität bei Einrichtung der Online-ID prüft. Denn auf diese Erstprüfung beziehen sich später alle Online-Nachweise.
- Dann muss geklärt sein, wie gut die Online-ID gegen einen Identitätsdiebstahl geschützt ist. Selbst eine Zwei-Faktor-Authentifizierung, mit der sich der Auskunftssuchende bei dem Identity-Provider angemeldet hat, um seine Identität zu bestätigen, lässt sich mitunter austricksen.
- Schließlich macht es die Vielzahl an verschiedenen Online-IDs schwierig, Identitätsnachweise darüber abzubilden. Denn ein Unternehmen müsste viele ID-Dienste unterstützen.

Besser wäre also eine ID, die jede Bürgerin und jeder Bürger und damit jede Kundin und jeder Kunde in Deutschland hat. Hier kommt der Personalausweis ins Spiel.

Online-Funktion des Personalausweises

Über zehn Jahre nach der Einführung des elektronischen Personalausweises ist das Interesse an der Online-Funktion grundsätzlich groß, so eine Umfrage des Digitalverbands Bitkom. Sieben von zehn Bundesbürgern (69 %) würden den elektronischen Personalausweis nutzen, um sich bei digitalen Behördengängen zu identifizieren. Noch ist die Nutzung dieser eID aber eher gering.

Auf Grundlage des Onlinezugangsgesetzes (OZG) sollen 575 Verwaltungsdienstleistungen bis Ende 2022 online zugänglich sein. Die Online-Funktion des Personalausweises soll nach den Plänen des Bundes zukünftig einfacher gestaltet und an den Nutzerbedürfnissen ausgerichtet werden.

Nutzer und Nutzerinnen eines NFC-fähigen Smartphones könnten nach Installation der AusweisApp2 (www.ausweisapp.bund.de/ausweisapp2/) die Online-Ausweisfunktion des Personalausweises heute schon deutlich stärker einsetzen. Daher wäre gerade die Verbindung NFC-Funktion eines Smartphones + AusweisApp2 + Online-Ausweisfunktion des Personalausweises ein vielversprechender Weg, um Identitätsnachweise digital zu erbringen.

In Zukunft geht dann das Online-Ausweisen direkt im Smartphone ohne die Ausweiskarte, so das Bundesinnenministerium, also mit einem Smartphone-basierten Personalausweis.

PRAXIS-TIPP

Noch hat sich kein digitaler Identitätsnachweis durchsetzen können. Unternehmen müssen also weiterhin mit verschiedenen Verfahren arbeiten, um die Identität bei Auskunftsersuchen zu kontrollieren. Es lohnt sich aber, die Online-Ausweisfunktion in Verbindung mit der AusweisApp2 und der NFC-Funktion des Smartphones im Auge zu behalten. Das könnte mittelfristig den digitalen Weg der Identitätsprüfung ebnen. Stellen Sie daher als Datenschutzbeauftragte/r diese Verfahren beispielsweise im Rahmen einer Schulung vor.

Oliver Schonschek, Dipl.-Phys., ist Technology Analyst mit Fokus auf IT-Sicherheit und Datenschutz.

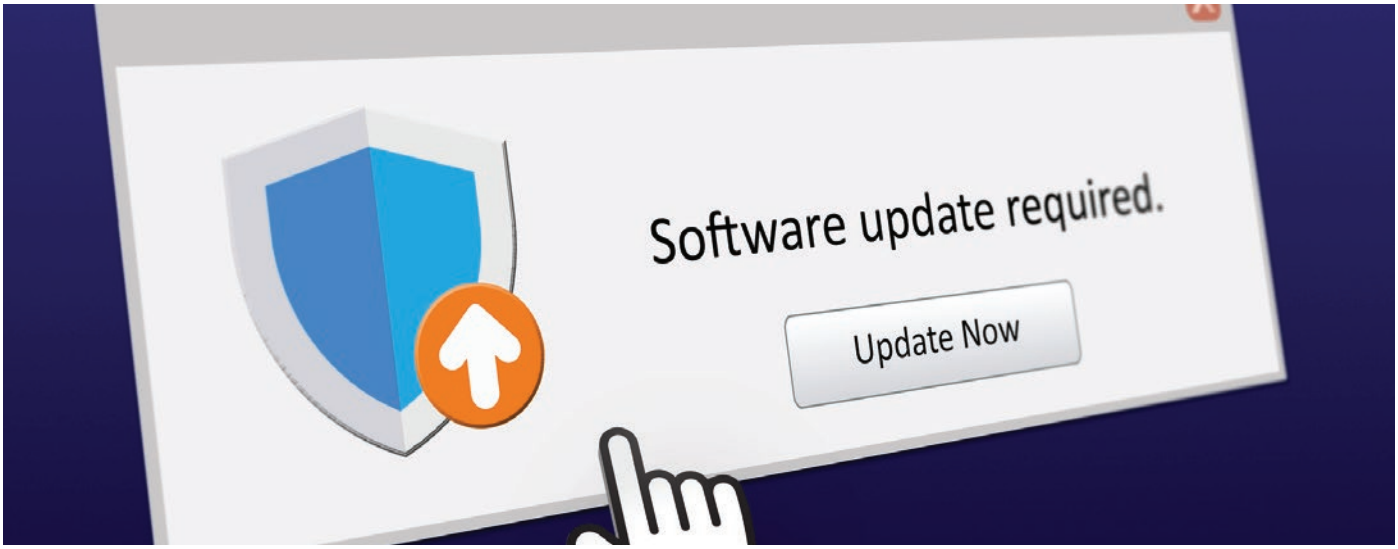


Bild: iStock.com/glegorly

Schnell tun sich Sicherheitslücken auf, wenn niemand Updates sorgfältig prüft

Datenschleuder GmbH oder sicheres Unternehmen?

In 10 Schritten zum richtigen Patchen und Updaten

Jeder kann nach Wartungsarbeiten plötzlich die Gehaltsabrechnung aller anderen Kolleginnen und Kollegen einsehen – was ist da bloß passiert? Lesen Sie, wie sich solche Datenschutzvorfälle umschiffen lassen.

In einem Betrieb können beschäftigte Personen mit ihrem individuellen Passwort ihre Gehaltsabrechnung ansehen. Dabei befinden sie sich in einer Liste mit allen anderen beschäftigten Personen, die ihrerseits alle ein anderes, frei gewähltes eigenes Passwort haben. Normalerweise kann also niemand mit seinem Passwort eine andere Gehaltsabrechnung einsehen.

Der Praxisfall: Alles auf „Masterpasswort“

Bei Wartungsarbeiten an diesem Teil des Programms stellt der Support die Passwörter alle auf „Masterpasswort“, um die Arbeiten bequem zu erledigen. Nicht geplant war hingegen, dass der Support vergisst, die Eigenschaft „Masterpasswort“ wieder in „Userpasswort“ zurück zu ändern. Damit wurde es grundsätzlich möglich, dass jeder alle Gehaltsabrechnungen einsehen konnte. Allerdings wusste das niemand.

Bei den nächsten routinemäßigen Wartungsarbeiten drei Monate nach dem ersten Vorfall fiel das Versäumnis auf. Der Support machte den Fehler sofort rückgängig. Fakt war: Für die letzten drei Monate konnten alle Beschäftigten alle Gehaltsmitteilungen einsehen. Eine klassische Schutzverletzung nach Art. 4 Nr. 12 Datenschutz-Grundverordnung (DSGVO).

Meldepflichtiger Datenschutzvorfall

Das Unternehmen informierte den Datenschutzbeauftragten (DSB). Sein Tipp: in der Protokollierung nachsehen, ob jemand den Fehler entdeckt und ausgenutzt hat. Tatsächlich hatte jedoch offenbar niemand diese Lücke erkannt. Keine einzige Gehaltsmitteilung war unbefugt angesehen worden. Allerdings reichte die Protokollierung nur zwei Monate zurück. Es blieb also eine Lücke von vier Wochen, für die sich nicht ausschließen ließ, dass jemand die Gehaltsmitteilungen unbefugt eingesehen hatte. Das machte die Meldung an die Aufsichtsbehörde unvermeidlich.

Die Ausgangslage: ungeklärte Zuständigkeiten = offene Flanken

Hätte sich dieser Datenschutzvorfall vermeiden lassen, und wenn ja, wie? Es geschieht immer wieder, dass der Support nach Sicherheits- →

Meist zahlreiche offene Fragen

Viele DSB werden feststellen, dass sie umso mehr offene Fragen haben, je tiefer sie in die Materie einsteigen. Vor allem werden sie beim Versuch, sich einen ersten Überblick zu verschaffen, feststellen, dass es etliche Fälle gibt, in denen Wartungszugriffe erfolgen, aber nur unzureichend protokolliert ist, was genau geschieht. Es kann durchaus sein, dass Sie schon in diesem Schritt einige offene Flanken entdecken, die möglicherweise auch zu Datenschutzverstößen geführt haben, die aber niemand entdeckt hat.

PRAXIS-TIPP

Auftraggeber gehen zu oft davon aus, dass der Dienstleister automatisch die erforderlichen Kontrollen vornimmt. Prüfen Sie also, ob das im Einzelfall Vertragsbestandteil ist oder nicht. Denn viele Verantwortliche glauben, dass sie mit Vergabe des Auftrags auch gleichzeitig die Überprüfung eingekauft haben. Ob das wirklich der Fall ist, und wenn ja, ob der Dienstleister dem auch zuverlässig nachkommt, steht häufig in den Sternen.

patches, Updates oder Wartungsarbeiten die Einstellungen nicht wieder so vornimmt, wie sie zuvor waren. So kommt es zu Schutzverletzungen, die zu einer Meldepflicht an die Datenschutzaufsichtsbehörde führen können.

Um solche offenen Flanken zu vermeiden, müssen die Eingriffe in die Software und ihre Einstellungen über dokumentierte Tests strukturiert ablaufen – gleich ob interne Mitarbeitende die Wartung vornehmen oder externe.

Wer führt Tests durch?

Normalerweise ist es Teil der Wartungsarbeiten oder der Sicherheitspatches, dass ausgewählte Nutzerinnen und Nutzer im Anschluss an die Arbeiten vor Freigabe testen, ob alle Einstellungen wieder so funktionieren wie zuvor. Das gilt auch für die Sicherheitseinstellungen. Oft erledigt diese Arbeiten der Support selbst und dokumentiert seine Tests.

Immer öfter sind jedoch externe Dienstleister für Support- und Wartungsarbeiten zuständig. Solange die beschäftigten Personen, die zuvor Support und Wartung durchgeführt haben, noch im Unternehmen sind, können sie nach Ende der Wartungsarbeiten prüfen, ob alles wie vorgesehen funktioniert und ob die Einstellungen wieder so sind, dass es nicht zu Datenschutzverletzungen kommen kann.

Das gilt jedoch nur, wenn diese fachkundigen Personen auch eingebunden sind und den Umfang der Veränderungen kennen. Oft ist das nicht mehr der Fall, v.a. je länger die Zeit der aktiven Mitarbeit zurückliegt.

Schlecht geplantes Outsourcing

Viel zu oft lässt sich beobachten, dass Betriebe bisher dafür zuständige Mitarbeiterinnen und Mitarbeiter anderweitig einsetzen, nachdem sie die Arbeiten ausgelagert haben. Ob sie zugleich daran gedacht haben, die erforderliche Prüfung ebenfalls an den externen Support auszulagern, ist angesichts der vielen Fälle, in denen es durch fehlende Regelungen zu Datenschutzverletzungen kommt, zumindest fraglich.

Dass sich intern oder beim externen Dienstleister jemand dafür zuständig fühlt, die erforderlichen Prüfungen durchzuführen, ist in vielen Fällen erfahrungsgemäß nicht gesichert.

10 Schritte zum richtigen Patchen und Updaten

1. Überblick verschaffen

Verschaffen Sie sich im ersten Schritt einen Überblick, für welche Anwendungen regelmäßig Patches, Updates oder ein Support erfolgen. Hierzu gehören Betriebssysteme, Office-Programme, Standardsoftware, Datenbanksysteme, Server, Maschinen und Anlagen sowie andere Geräte mit Internetanbindung wie Klimaanlage, Kaffeemaschinen usw.

Ist bereits ein vollständiges (!) und aktuelles (!) Inventar über informationstechnische Systeme vorhanden, haben Sie eine gute Grundlage für diesen Überblick. Lesen Sie dazu auch den Datenschutz-PRAXIS-Beitrag mit Checklisten-Download „In 20 Schritten zum Software-Inventar“ (https://ogy.de/software-inventar).

2. Wie ist die Wartung geregelt?

Bringen Sie als Nächstes in Erfahrung, wie die Wartung definiert ist.

- Erfolgt die Wartung über einen externen Dienstleister in einem Wartungsvertrag oder intern?
- Wird ad hoc gewartet?
- Ist Wartung im Vertrag gar nicht genannt, also ausgeschlossen?
- Wie erfolgen Reparaturen?
- Wer erhält in solchen Fällen Zugriff auf die Daten der Systeme?

3. Sicherheitseinstellungen prüfen

Prüfen Sie im nächsten Schritt, ob Sie für die jeweilige Anwendung die erforderlichen Sicherheitseinstellungen hinsichtlich des Datenschutzes ausfindig machen können und ob diese Einstellungen vollständig und aktuell sind.

Dabei ist nicht so sehr die Frage, ob Sie als DSB diese Einstellungen kennen. Es geht vielmehr darum, herauszufinden, ob es überhaupt jemanden gibt, der im Umfeld des zu wartenden informationstechnischen Systems tätig ist und weiß, wann wer wie patcht, updatet und wartet.

Am besten ergänzen Sie das Inventar aus dem ersten Überblick um die bekannten Wartungsintervalle und die Dienstleister, die die Wartung

vornehmen. So erhalten Sie einen Plan, wann welche Wartungen durchzuführen sind. Das ist dann die Grundlage, um kontrollieren zu können, wie konkret die Wartung erfolgt und ob die Beteiligten dabei die Datenschutzbestimmungen einhalten.

4. Verantwortlichkeiten definieren

Prüfen Sie zusammen mit den Fachverantwortlichen, ob es für die Patches, Updates und den Support definierte Verantwortlichkeiten gibt. Wer ist dafür zuständig,

- den Patch freizugeben,
- die Updates einzuspielen oder
- den Support auf die Anwendung zu lassen?

Es kann sein, dass für diese Tätigkeiten keine zentrale Verantwortung vorliegt, sondern zahlreiche Personen eingebunden sind. Ergänzen Sie also das Inventar über informationstechnische Systeme um die Personen, mindestens aber um die Funktionen, die für Patches, Updates oder den Support verantwortlich sind.

5. Auftragsverarbeitung erkennen und rechtssicher machen

Prüfen Sie zusammen mit den Fachverantwortlichen, ob ein Vertrag zur Auftragsverarbeitung (AV) gemäß Art. 28 DSGVO erforderlich ist, und wenn ja, ob die Beteiligten ihn korrekt geschlossen haben. In viel zu vielen Fällen werden Sie feststellen, dass zwar Wartungsverträge vorliegen, aber kein Vertrag zur Auftragsverarbeitung, obwohl der Dienstleister auf personenbezogene Daten zugreifen kann.

6. Leistungswege erkennen und protokollieren

Prüfen Sie für jeden Patch, für jedes Update und für den Support, wie die Leistung erbracht wird. Also ob jeweils der Impuls aus dem Unternehmen kommt, ob ein automatisierter Zugriff möglich ist oder ob fachkundiges externes Personal den jeweiligen Eingriff so begleitet, dass zu jeder Zeit ein Unterbrechen möglich ist. Außerdem ist wichtig, festzuhalten, wie die Arbeiten protokolliert werden.

1. Der automatisierte Direktzugriff: Es gibt Fälle, in denen die technische Überwachung der zu wartenden Geräte automatisiert erfolgt. Dabei hat der Dienstleister für den Support einen permanenten Zugriff auf die Daten. Möglicherweise erfolgt im Hintergrund sogar eine automatisierte Auswertung, die zu einem Alarm führt, wenn die Abweichungen in kritische Bereiche hineinkommen. Das kann dazu führen, dass der Support-Techniker vor Ort auftaucht, obwohl die Maschine noch läuft. Es steht dann zu erwarten, dass aufgrund der technischen Daten der Schaden bald eintreten wird.
2. Die Störungsmeldung: In anderen Fällen erfolgt der Support so, dass bei einer Störung ein Wartungstechniker beim Dienstleister eine Meldung erhält. Der Techniker lässt sich entweder den Störfall schildern. Oder er greift direkt auf eine Software zu, die beim Unternehmen auf dem System oder der Maschine installiert ist, und liest aus, welcher Schaden eingetreten ist. In diesem Fall erfolgt der Wartungszugriff nicht automatisiert, sondern erst nach Freigabe aus dem Unternehmen heraus. Das kann zu unliebsamen Arbeitsunterbrechungen führen. Deshalb wird diese Methode nicht mehr so oft angewendet.
3. Das klassische Wartungsintervall: Nach wie vor gibt es auch Supportfälle, in denen Betriebe das standardmäßige Wartungsintervall abwarten, und dann ein Techniker vor Ort die Wartung ausführt.

Bei Software-Updates, bei Software-Support und bei Software-Patches geht der Wartungsvorfall in der Regel vom Hersteller der Software aus. In diesem Fall können sämtliche Rechner des Unternehmens betroffen sein. Normalerweise finden solche Wartungsarbeiten außerhalb der Arbeitszeit statt. Das hält die Störungen im normalen Tagesgeschäft in der Regel so gering wie möglich.

Wichtig ist, die jeweiligen Leistungswege zu erkennen und so weit zu protokollieren, dass sich überprüfen lässt, ob bei der Wartung, beim Patchen oder beim Updaten die Datenschutzbedingungen eingehalten wurden.

7. Sicherheitseinstellungen wiederherstellen

Prüfen Sie, wie die Fachabteilung oder der beauftragte Dienstleister sicherstellt, dass nach Patches oder Updates die Sicherheitseinstellungen zuverlässig noch vorhanden oder wiederhergestellt worden sind. →

BEISPIEL

Ein Beispiel zur Auftragsverarbeitung: Am Bedienterminal einer Säge in der Produktion müssen sich zu Schichtbeginn die beschäftigten Personen anmelden, die während dieser Schicht mit der Säge arbeiten. Somit sind zumindest Name und Arbeitszeiten dieser Personen bekannt. Erfolgt hier ein Wartungszugriff von außerhalb, fragt der Dienstleister mindestens diese Daten von außen mit ab. Damit sind Sie schon mitten im Datenschutz angekommen. Je nachdem, wie der Umfang des Zugriffs geregelt ist, können Sie jetzt anhand der üblichen Kriterien prüfen, ob es sich um eine Auftragsverarbeitung handelt. In der Folge prüfen Sie, ob die Beteiligten die AV-Verträge korrekt abgefasst haben und ob regelmäßig überprüft wird, dass die dabei vereinbarten technischen und organisatorischen Maßnahmen noch gelten.

Sicherheitseinstellungen testen

Ist der Patch erfolgt, das Update eingespielt oder der Wartungsfall abgeschlossen, gilt es, vor der Wiederaufnahme der Produktivtätigkeit zu testen, ob die aus den vorherigen Schritten bekannten Sicherheitseinstellungen wieder so vorgenommen wurden, wie sie davor waren, und ob bei neuen Funktionen die aus Sicht des Datenschutzes erforderlichen Sicherheitseinstellungen aktiv sind.

Das können durchaus Testreihen sein, die mehrere Stunden in Anspruch nehmen. Schon allein deswegen sollten diese Arbeiten nicht am laufenden System, quasi am offenen Herzen, geschehen, sondern außerhalb des laufenden Systems. Und erst nach Tests geht das Ganze wieder live. Üblicherweise gibt es für diese Fragestellung Lösungen, die bei den jeweiligen Herstellern bekannt sind.

8. Kontrollen durchführen

Sind für jeden Patch, jedes Update und den Support Regelungen vorhanden, die eine Prüfung erlauben, ob die Sicherheitseinstellungen nach Abschluss der Arbeiten wieder hundertprozentig funktionieren, führen Sie stichprobenartig Kontrollen durch, wie die Zuständigen die Sicherheitseinstellungen vorgenommen haben, wie diese geprüft und wie diese dokumentiert werden. Das ist originärer Teil Ihrer Überwachungsaufgabe als DSB.

Diese stichprobenartigen Kontrollen müssen Sie immer dann ausweiten, wenn es zu einer nicht mehr tolerierbaren Fehlerquote kommt. Dokumentieren Sie Ihre stichprobenartigen Kontrollen. Kommt es zu Abweichungen von den definierten Leistungswegen, klären Sie, woran dies im Einzelnen lag und wie sich künftig Abweichungen vermeiden lassen.

9. Für Sensibilisierung sorgen

Prüfen Sie, ob Sensibilisierungsmaßnahmen für diejenigen Personen erforderlich sind, die zum einen Patches, Updates und Support begleiten und zum anderen die Überprüfungen vorzunehmen haben. Stellen Sie sicher, dass Sie als DSB in Zweifelsfällen eingeschaltet werden.

In aller Regel, v.a. aber dann, wenn eine ISMS-Zertifizierung vorhanden ist, also eine Zertifizierung des Informationssicherheitsmanagementsystems nach ISO/IEC 27001, liegt der Schwerpunkt im Zusammenhang mit Patches, Updates und Support auf der Informationssicherheit. Datenschutz spielt dann in der Wahrnehmung eine eher nachrangige Rolle. So gesehen ist es auf alle Fälle sinnvoll, diejenigen beschäftigten Personen, möglicherweise aber auch Externe, die das Patchen, die Updates oder den Support begleiten, mit den besonderen Bedingungen des Datenschutzes in diesem Zusammenhang vertraut zu machen.

PRAXIS-TIPP

Nehmen Sie Ihre Prüfungsergebnisse zum Patchen, Updaten und für den Support in Ihren Bericht auf. Da Fehler in diesen Bereichen in aller Regel zu Datenschutzverletzungen führen, egal ob sie intern erkannt oder von außen herangetragen werden, ist es unabdingbar, dass die Verantwortlichen ein Gefühl dafür bekommen, wie mit diesen Leistungsdaten umzugehen ist.

Praxisbeispiele, die sich immer wieder hier im Daten-Schluss, im Internet oder in einschlägigen Foren finden wie etwa das Eingangsbeispiel, leisten hierbei gute Dienste.

10. Datenschutzrichtlinie erstellen

Erstellen Sie, sofern noch nicht vorhanden, eine Datenschutzrichtlinie für das richtige Patchen, Updaten und für den Support. Die Datenschutzrichtlinie sollte alle hier aufgezeigten Punkte umfassen. Sie klärt also,

- wer für welche Bereiche verantwortlich ist,
- wie die Verantwortung wahrzunehmen ist,
- wie die Leistungswege sind,
- wie Sicherheitseinstellungen zu definieren sind,
- wie sich kontrollieren lässt, dass die Sicherheitseinstellungen zuverlässig wiederhergestellt sind, und
- wie bei Abweichungen vorzugehen ist.

Diese Datenschutzrichtlinie kann durchaus mehrere Seiten umfassen und zugleich als Grundlage für die Sensibilisierungen dienen.

Zusammenfassung

Mit großer Wahrscheinlichkeit ist der Bereich des Patchens, Updatens und der Begleitung der Wartungsarbeiten für viele Datenschutzbeauftragte kein vertrautes Feld. Zumal in der Regel das Fachpersonal nicht mehr zur Unterstützung zur Verfügung steht, wenn das Unternehmen die Aufgaben bereits in die Cloud verlegt hat.

- Erarbeiten Sie sich das Know-how entweder neu oder nehmen Sie möglichst rasch mit Kolleginnen und Kollegen Kontakt auf, die früher für die Updates zuständig waren, sofern sie noch im Unternehmen sind.
- Zieht der Verantwortliche Sie rechtzeitig hinzu, bevor er alle Aufgaben an einen externen Dienstleister auslagert, empfehlen Sie, das interne Know-how zu erhalten und zu dokumentieren.
- Ihr zentrales Arbeitsmittel ist eine Software-Inventarliste, die Sie um die Informationen ergänzen, die Sie zusätzlich für Ihre Kontrollen benötigen.

Eberhard Häcker ist seit vielen Jahren als externer Datenschutzbeauftragter tätig. So kennt er die typischen Schwachstellen in Organisationen in- und auswendig.

Bild: iStock.com/Julia Lemba

Datenschutzaufsicht Baden-Württemberg

Überwachung privater Parkflächen

Immer mehr Privatunternehmen lassen ihren Kundenparkplatz oder ihr Kundenparkhaus durch einen Dienstleister überwachen. Parkt dort jemand, der dazu nicht berechtigt ist, oder überschreitet jemand die zulässige Parkdauer, bekommt er eine Rechnung wegen „Falschparkens". Die Datenschutzaufsicht Baden-Württemberg bewertet dies aus Sicht des Datenschutzes wie folgt:

- Wer einen privaten Stellplatz oder ein privates Parkhaus benutzt, schließt „stillschweigend" mit dem Betreiber einen Vertrag ab. Falls das im Vertrag vorgesehen ist, muss der Fahrer eine Vertragsstrafe entrichten, wenn er die geltende Parkordnung nicht einhält.
- Das Überwachungsunternehmen kann sich die Daten des Fahrzeughalters über das Kraftfahrtbundesamt oder die Zulassungsstelle beschaffen.
- Das Unternehmen kann die Daten nutzen, um den Halter des fraglichen Fahrzeugs anzuschreiben und danach zu fragen, ob er den „Parkverstoß" begangen hat bzw. wer der Fahrer war.
- Nach der jüngeren Rechtsprechung des Bundesgerichtshofs muss der Halter „im Rahmen des ihm Zumutbaren" dem Unternehmen mitteilen, wer als Fahrer infrage kommt. Er muss, wenn er nicht weiß oder wissen sollte, wer das Fahrzeug zum fraglichen Zeitpunkt benutzt hat, zumindest so konkrete Angaben machen, dass es dem Unternehmen möglich ist, den „Vertragspartner" zu ermitteln. Tut der Halter das nicht, muss er die Vertragsstrafe meist selbst bezahlen.
- Nach Abschluss eines Inkassoverfahrens muss das Überwachungsunternehmen die Daten der betroffenen Person grundsätzlich löschen. Die weitere Speicherung für einen angemessenen Zeitraum ist nur zulässig, wenn die Geschäftsbedingungen vorsehen, dass im Wiederholungsfall eine höhere „Gebühr" erhoben wird.

Quelle: Datenschutzaufsicht Baden-Württemberg, 36. Tätigkeitsbericht für das Jahr 2020, Seiten 110/111, abrufbar unter https://ogy.de/tb-bawue-2020.

Europarat

Richtlinien zur Gesichtserkennung

Richtlinien dafür, wie mit Maßnahmen der Gesichtserkennung umzugehen ist, hat der Beratende Ausschuss zur Datenschutzkonvention 108 des Europarats veröffentlicht. Adressaten dieser Richtlinien sind in erster Linie die Gesetzgeber der Mitgliedstaaten des Europarats, ferner Software- und Systementwickler, die an Software und Produkten zur Gesichtserkennung arbeiten. Außerdem wendet sie sich an Unternehmen, die Systeme der Gesichtserkennung einsetzen.

Die Richtlinien sind rechtlich nicht verbindlich. Gleichwohl sollten v.a. international tätige Unternehmen über ihren Inhalt orientiert sein. Die Richtlinien bilden den aktuellen Stand der europaweiten Diskussion recht zuverlässig ab. Das Dokument mit dem Titel „Guidelines on Facial Recognition" des Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data / Convention 108" trägt das Datum 28. Januar 2021 und hat einen Umfang von 16 Seiten. Es ist (bisher nur auf Englisch) abrufbar unter https://ogy.de/guidelines-on-facial-recognition.

Datenschutzaufsicht Hamburg

Zwangsgeld bei Auskunftsverweigerung

Die Diskussion über die Folgen von Datenschutzverstößen konzentriert sich sehr stark auf die Geldbußen gemäß Art. 83 DSGVO. Übersehen wird dabei oft, dass die Aufsichtsbehörden auch verwaltungsrechtliche Druckmittel haben, die teuer werden können. Sie kommen v.a. zur Anwendung, wenn ein Unternehmen Auskünfte gegenüber der Datenschutzaufsicht mehrfach verweigert. Ein Beispiel hierfür ist ein Fall aus Hamburg.

Das US-Unternehmen Clearview AI Inc. bietet eine App zur Erkennung von Gesichtern an. Aufgrund zahlreicher Beschwerden eröffnete die Datenschutzaufsicht Hamburg ein Verwaltungsverfahren. Ziel war, den Sachverhalt zu klären. Auskunftsersuchen der Aufsichtsbehörde beantwortete das Unternehmen aus Sicht der Aufsicht nur ausweichend und unvollständig. Dies führte dazu, dass die Behörde schließlich einen „Auskunftsheranziehungsbescheid" erließ. Darin setzte sie ein Zwangsgeld in Höhe von 10.000 € fest.

Solche Zwangsgelder sind nicht in der DSGVO geregelt. Rechtsgrundlage sind vielmehr die Regelungen über die Verwaltungsvollstreckung im jeweiligen Bundesland. Für Hamburg findet sich eine solche Regelung in § 14 des Hamburgischen Verwaltungsvollstreckungsgesetzes (abrufbar unter https://ogy.de/VwVGHA). Die Festsetzung eines solchen Zwangsgelds soll Druck ausüben und bewirken, dass ein Unternehmen die geforderte Auskunft erteilt. Eine Geldbuße wegen Verletzung der Auskunftspflicht kann die Aufsichtsbehörde unabhängig davon zusätzlich festsetzen.

Quelle: Datenschutzaufsicht Hamburg, Tätigkeitsbericht 2020, Seiten 105–107. Der Bericht ist abrufbar unter https://ogy.de/tb-lfd-hamburg-2020.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken. Er beschäftigt sich seit Jahren mit dem Datenschutz in Unternehmen und Behörden.

Bild: iStock.com/Morsa Images

Was sagen die gesetzlichen Vorgaben zur IT-Sicherheit im Gesundheitsbereich in Deutschland aktuell? Hier tut sich tatsächlich gerade einiges.

Sicherheit der Verarbeitung

IT-Sicherheit in Krankenhäusern und Arztpraxen

Großes oder kleines Krankenhaus, große oder kleine Arztpraxis? Je nachdem gelten andere gesetzliche Vorgaben für die IT-Sicherheit. Die Richtlinien, Muster und Priorisierungen sind auch für weitere schweigepflichtige Berufe und kleine Unternehmen interessant.

Durch die Festlegungen der BSI-Kritisverordnung (BSI-KritisV) vom 22. April 2016 (BGBL I, 598; geändert BGBl I, 1903) fallen Kliniken mit mehr als 30.000 stationären Aufnahmen pro Jahr unter die KRITIS-Regeln im BSI-Gesetz (BSIG).

Große Krankenhäuser

Danach müssen diese Kliniken mindestens alle zwei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachweisen, dass sie angemessene organisatorische und technische Vorkehrungen treffen, um Störungen zu vermeiden bei der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich sind, die sie betreiben.

Die Ergebnisse einschließlich der aufgedeckten Sicherheitsmängel müssen sie an das BSI übermitteln (§ 8a BSIG).

Darüber hinaus hat die deutsche Krankenhausgesellschaft einen branchenspezifischen Sicherheitsstandard (B3S) für die Informationssicherheit im Krankenhaus erstellt und mit dem BSI abgestimmt. Er ist gemäß Feststellungsbescheid des BSI vom 22.10.2019 geeignet, um die Anforderungen nach § 8a Abs. 1 BSIG in Krankenhäusern zu gewährleisten. Damit ist ein Sicherheitsstandard für die großen Krankenhäuser verfügbar (abrufbar unter https://ogy.de/downloads-b3s; Orientierungshilfe des BSI zu den Nachweisen nach § 8a Abs. 1 BSIG siehe https://ogy.de/oh-nachweise-bsig).

Kleine Krankenhäuser

Das Patientendaten-Schutz-Gesetz vom 14. Oktober 2020 (BGBl. I, 2115) hat mit § 75c Anforderungen an die IT-Sicherheit in Krankenhäusern, die keine kritische Infrastruktur sind, in das Sozialgesetzbuch (SGB) V aufgenommen. Diese Regelungen sind ab 1. Januar 2022 anzuwenden.

Krankenhäuser müssen nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen treffen, um Störungen zu vermeiden bezüglich der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Dies kann insbesondere durch die Anwendung des B3S für Krankenhäuser erfolgen. Anpassungen an den Stand der Technik müssen mindestens alle zwei Jahre erfolgen.

Praxen

Das Digitale-Versorgung-Gesetz (DVG) vom 9. Dezember 2019 hat § 75b in das SGB V eingefügt. Danach mussten die Kassenärztlichen Bundesvereinigungen (Kassenärztliche Bundesvereinigung = KBV und Kassenzahnärztliche Bundesvereinigung = KZBV) bis zum 30. Juni 2020 in einer Richtlinie die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung festlegen.

Die Richtlinien sind, wenn auch verspätet, Anfang 2021 in Kraft getreten (abrufbar unter https://hub.kbv.de/site/its und www.kzbv.de/it-sicherheitsrichtlinie.1475.de.html).

Die beiden wörtlich identischen Richtlinien sind mit dem BSI abgestimmt. Sie

<table>
<tr><td colspan="2"></td><td>Kleine Krankenhäuser
Bis zu 30.000
stationäre Fälle/Jahr</td><td>Große Krankenhäuser
Mehr als 30.000
stationäre Fälle/Jahr</td></tr>
<tr><td colspan="2"></td><td>angemessene Vorkehrungen
nach § 75c SGB V
insb. auch B3S Krankenhaus
(Umsetzung ab 1.1.2022)</td><td>§ 8a Abs. 1 BSIG oder
B3S Krankenhaus oder
ISO 27001
(erstmalig bis zum 30.6.2019)</td></tr>
<tr><td>Kleine Praxis
Bis zu 5 Personen ständig mit Datenverarbeitung betraut</td><td>Mittlere Praxis
6 bis 20 Personen ständig mit Datenverarbeitung betraut</td><td>Große Praxis
Mehr als 20 Personen ständig mit Datenverarbeitung betraut oder sehr umfangreiche DV</td><td></td></tr>
<tr><td colspan="3">Anlagen 1, 5 und, falls entsprechende Großgeräte vorhanden, Anlage 4 der RL nach § 75b SGB V</td><td></td></tr>
<tr><td></td><td colspan="2">Zusätzlich Anlage 2 der RL</td><td></td></tr>
<tr><td colspan="2"></td><td>Zusätzlich Anlage 3 der RL</td><td></td></tr>
<tr><td colspan="3">Umsetzung je nach Vorgabe ab 1.4.2021, 1.7.2021, 1.1.2022 oder 1.7.2022</td><td></td></tr>
<tr><td colspan="3">Alternativ: Vorkehrungen nach § 8a Abs. 1 BSIG oder B3S Krankenhaus</td><td></td></tr>
</table>

Übersicht über die Vorgaben für Krankenhäuser und Praxen zur Umsetzung angemessener organisatorischer und technischer Vorkehrungen, um die IT-Sicherheit zu gewährleisten

müssen jährlich in Zusammenarbeit mit dem BSI an den Stand der Technik und an das Gefährdungspotenzial angepasst werden. Darüber hinaus müssen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bundesärztekammer, die Bundeszahnärztekammer, die Deutsche Krankenhausgesellschaft und die für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbände aus dem Bereich der Informationstechnologie im Gesundheitswesen bei der Erstellung und Anpassung angehört werden.

Modulare IT-Sicherheitsmaßnahmen

Die IT-Sicherheitsmaßnahmen sind modular nach Praxisgröße und Ausstattung der Praxis (Großgeräte) gruppiert. Sie gliedern sich in die Gruppen

- Software und Internet,
- Hardware inkl. Netz sowie
- Großgeräte & Telematik (Konnektoren).

Die Maßnahmen geben abstrakt vor, was die Praxen bedenken müssen. Während eine „Regelmäßige Datensicherung" (A1.14 = Anlage 1 Nr. 14) für alle Praxisgrößen Pflicht ist, empfehlen die Richtlinien eine „Datenträgerverschlüsselung" (A3.10) nur für Wechseldatenträger in Großpraxen. Eine Verschlüsselung von Patientendaten müsste für alle Praxen Pflicht sein. Eine Verschlüsselung in der Cloud ist für alle Pflicht (A1.10). Die Hälfte der zusätzlichen Maßnahmen für die Großpraxen beziehen sich auf Mobile Device Management.

Für zwei Bereiche fordern die Maßnahmen, Richtlinien zu erstellen: für den Einsatz mobiler Geräte (A2.6, A2.8 und A3.1) und für die Nutzung von Wechseldatenträgern (A2.10). Für beide Bereiche gibt es Musterrichtlinien auf der Themenseite der KBV. Für die Erstellung eines Netzwerkplans (A1.33) findet sich ebenfalls ein Muster, allerdings nur als PDF-Datei. Außerdem seien die jeweiligen FAQ auf den Informationsseiten der KBV und der KZBV dringend empfohlen (https://ogy.de/kbv-faq, https://ogy.de/kzbv-faq).

Zertifizierung

Eine dritte Richtlinie regelt die Zertifizierung von Personen, die im Rahmen von Dienstleistungen die Praxen bei der Umsetzung der Richtlinie sowie bei zukünftigen Anpassungen unterstützen oder die die Geräte zur Verbindung mit der Telematikinfrastruktur installieren oder warten. Die Richtlinie beschreibt die fachlichen Voraussetzungen, die Prüfung und eine Anerkennung von anderen Zertifizierungen (z.B. BSI Grundschutz-Auditor).

Optimierungen

Die Formulierungen in den Erläuterungen unterteilen die Maßnahmen für Praxen in „muss"- und „sollte"-Regeln. Hier ist eine sprachliche Überarbeitung sinnvoll. Denn „sollte" ist immer vorhanden, „muss" fehlt manchmal (z.B. A1.1).

Es wäre generell sicherlich sinnvoll, die Regelungen für Krankenhäuser und Praxen zu vereinheitlichen. Denn die Praxen müssen ebenfalls die technisch-organisatorischen Aspekte des Datenschutzes berücksichtigen. So geben die Richtlinien für Praxen z.B. keinen Schutz der Vertraulichkeit durch Verschlüsselung bei der Dateiablage vor. Auch müssten die Vorgaben datenschutzkonforme Begriffe (z.B. schreibt A1.18 „persönliche Daten") verwenden.

Prof. Dr. Rainer W. Gerling ist Autor und Referent sowie stellvertretender Vorsitzender des Vorstands der GDD e.V. Er lehrt IT-Sicherheit an der Hochschule München.

Bild: iStock.com/Drazen Zigic

Die Sozialauswahl ist strikt auf vier Kriterien beschränkt: die Dauer der Betriebszugehörigkeit, das Lebensalter, die Unterhaltspflichten und eine etwaige Schwerbehinderung

Fallstricke vermeiden

Datenschutz & Sozialauswahl: Darauf müssen Sie achten

Betriebsbedingte Kündigungen sind derzeit keine traurigen Ausnahmen, sondern praktisch Tagesgeschäft. Auch wenn DSB im Auswahlverfahren keine zentrale Rolle spielen, ist ihre fachkundige begleitende Beratung angesichts der Sensibilität der verarbeiteten Daten wichtig.

Die Sozialauswahl ist ein besonderes Auswahlinstrument im Rahmen betriebsbedingter Kündigungen. Sind Arbeitgeber gezwungen, aus mehreren vergleichbaren Beschäftigten diejenigen auszuwählen, denen gekündigt werden soll, so müssen sie deren soziale Schutzbedürftigkeit berücksichtigen.

Rechtlich drohen viele Stolpersteine. Denn eine betriebsbedingte Kündigung ist unwirksam, wenn der Arbeitgeber die gesetzliche Sozialauswahl gar nicht oder falsch durchgeführt hat. Auch datenschutzrechtlich haben Verantwortliche bei der Sozialauswahl einiges zu beachten – verarbeiten sie doch u.a. besondere Kategorien personenbezogener Daten nach Art. 9 Datenschutz-Grundverordnung (DSGVO).

Welche personenbezogenen Daten sind betroffen?

Das Kündigungsschutzgesetz sieht in § 1 Abs. 3 vor, dass neben der Dauer der Betriebszugehörigkeit das Lebensalter, etwaige Unterhaltspflichten und ggf. bestehende Schwerbehinderungen eines Arbeitnehmers Einfluss auf die Sozialauswahl haben. So erhalten Beschäftigte mit einer langen Betriebszugehörigkeit, einem höheren Lebensalter und mehreren nachweisbaren Unterhaltspflichten mehr Punkte auf ihr Sozialkonto als Beschäftigte, auf die das Gegenteil zutrifft. Je mehr Punkte auf dem Sozialkonto verbucht sind, desto unwahrscheinlicher ist die zeitnahe betriebsbedingte Kündigung.

Je größer die zu erwartende Kündigungswelle ist, umso umfangreicher fällt die nötige Datenzusammenstellung im Rahmen der Sozialauswahl aus. Nicht selten entstehen auf diesem Weg umfangreich(st)e Excel-Tabellen, die zahlreiche brisante Details zu den Beschäftigten im Unternehmen enthalten – möglicherweise auch solche, die im Rahmen der Sozialauswahl gar nicht relevant sind.

Datenschutzgrundsätze beachten

Wie so oft sind daher auch im Rahmen der Sozialauswahl die Datenschutzgrundsätze von Bedeutung:

- die Rechtmäßigkeit und Transparenz der Verarbeitung,
- die strikte Zweckbindung der gesammelten Daten,
- die Beachtung des Grundsatzes der Datenminimierung und
- die Speicherbegrenzung.

Auch muss ein strenges Berechtigungskonzept nach dem „Need-to-know-Prinzip" sicherstellen, dass nur diejenigen Personen auf die Datensammlung zugreifen, die diesen Zugriff zwingend benötigen, um ihre Tätigkeit auszuüben.

Rechtsgrundlagen der Sozialauswahl

Rechtliches Gestaltungsmittel, um die Sozialauswahl umzusetzen, ist der sogenannte Sozialplan. Nach § 112 Abs. 1 Satz 3 BetrVG wirkt der Sozialplan wie eine Betriebsvereinbarung. Er bildet somit hinsichtlich der Verarbeitung von Beschäftigtendaten – einschließlich besonderer Kategorien personenbezogener Daten nach

ACHTUNG!

So verführerisch es auch wirken mag, neben den vier vorgegebenen Datenkategorien weitere vermeintlich relevante Daten von Beschäftigten heranzuziehen, so wäre dies jedenfalls nicht von der Rechtsgrundlage gedeckt.

Art. 9 DSGVO – eine Rechtsgrundlage im Sinne von § 26 Bundesdatenschutzgesetz (BDSG) in Verbindung mit Art. 88 DSGVO.

Transparenz- & Informationspflichten

Um den gesetzlich vorgeschriebenen Transparenz- und Informationspflichten nachzukommen, empfiehlt es sich, die Beschäftigten in geeigneter Art und Weise – etwa per Anschreiben, Aushang am Schwarzen Brett oder über das Intranet, soweit für jeden Beschäftigten die Möglichkeit der Kenntnisnahme besteht – über das geplante Prozedere aufzuklären.

Besonderes Augenmerk ist dabei auf die in Art. 13 DSGVO enthaltenen Vorgaben zu richten. Inhaltliche Schwerpunkte bilden der Zweck der Verarbeitung, die vorgesehene Speicherdauer der verarbeiteten Daten, die Darlegung bestehender Zugriffs- bzw. Einsichtsrechte sowie die Aufklärung über die Betroffenenrechte nach Art. 15 ff. DSGVO.

Grundsatz der Datenminimierung

Um die für die Sozialauswahl relevanten Datenkategorien im Rahmen betriebsbedingter Kündigungen zweifelsfrei einem bestimmten Beschäftigten zuordnen zu können, ist es erforderlich, weitere personenbezogene Daten zu verarbeiten. Hierzu zählen klassischerweise der Name, die Personalnummer oder die Abteilung der Beschäftigten. Um dem Grundsatz der Datenminimierung zu genügen, muss die Erweiterung der Datenkategorien, die für die Sozialauswahl relevant sind, so datensparsam und pseudonymisiert wie möglich erfolgen. So ist z.B. eine Personalnummer dem vollständigen Namen des Beschäftigten stets vorzuziehen.

Zweckbindung und Speicherdauer

Der Sozialplan verfolgt den Zweck, zukunftsbezogene ausgleichsfähige wirtschaftliche Nachteile, die durch die betriebsbedingte Kündigung entstehen, auszugleichen bzw. abzumildern. Obwohl in der Personalabteilung oftmals bereits Datenbestände vorhanden sein dürften, die für die Sozialauswahl relevant sind, dient die vollständige Übersicht aller nötigen Daten nebst Bewertungspunkten allein dem Prozess selbst. Sie darf nicht anderweitig verwendet werden.

Ist der Zweck – also die ordnungsgemäße Durchführung der Sozialauswahl im Rahmen der betriebsbedingten Kündigungen – erreicht, so ist die Verarbeitung der zusammengestellten Daten zunächst einzuschränken und nach Ablauf etwaiger Klage- und sonstiger gesetzlicher Aufbewahrungsfristen zu löschen.

Grundsatz der Richtigkeit

Schließlich liegt besonderes Augenmerk auf dem Grundsatz der Richtigkeit personenbezogener Daten. Das gilt v.a. dann, wenn sich Angaben über Unterhaltspflichten oder eine Schwerbehinderung vom Arbeitgeber unbemerkt geändert haben, die Informationen aber entscheidend sein können, um die Sozialauswahl ordnungsgemäß durchzuführen.

Arbeitgeber müssen den Beschäftigten daher – mit ausreichend Vorlauf und unter Einhaltung der Informationspflichten – Gelegenheit geben, die Richtigkeit bzw. die Vollständigkeit der für sie relevanten Datenkategorien sicherzustellen. Empfehlen Sie hierfür aus Gründen der Datensicherheit unbedingt die Schriftform statt der elektronischen Form.

Sind Nachweise über bestimmte Parameter erforderlich, wie z.B. für bestehende Unterhaltspflichten, so sollten die Beschäftigten diese ebenfalls in Papierform beim zuständigen Sachbearbeiter in der Personalabteilung einreichen. Das Anfertigen von Kopien oder Scans solcher Nachweise darf nur dann erfolgen, wenn es tatsächlich erforderlich ist.

Raten Sie den Beschäftigten hinsichtlich der Nachweise zu besonderen Kategorien personenbezogener Daten, wie z.B. etwaiger Schwerbehinderungen, sie persönlich bei der Schwerbehindertenvertretung einzureichen, nicht bei der Personalabteilung.

PRAXIS-TIPP

In der Praxis hat sich gezeigt, dass es in Unternehmen, in denen betriebsbedingt Kündigungen anstehen, äußerst sinnvoll ist, alle mit dem Prozess befassten Einheiten in Sachen Datenschutz nochmals eingehend zu schulen. Weisen Sie auch ausdrücklich auf das hohe Vertraulichkeitslevel der Materie und die Verschwiegenheitspflichten hin.

Mitbestimmungsrechte

Betriebsrat: kein unbeschränkter Zugriff!

Im Hinblick auf etwaige Mitbestimmungsrechte des Betriebsrats müssen Verantwortliche darauf achten, dass der Betriebsrat zwar einen grundsätzlichen Anspruch hat, zu überprüfen, ob der Arbeitgeber die Sozialauswahl ordnungsgemäß durchführt bzw. ob er die im Sozialplan getroffenen Vereinbarungen einhält. Das umfasst aber keinesfalls das Recht, im Detail zu erfahren, welche Beschäftigten in welcher der Datenkategorien welche Bewertung erhalten haben. Interessant sind für den Betriebsrat allein die aggregierten Gesamtbewertungspunkte und das Rangverhältnis bzgl. etwaiger betriebsbedingter Kündigungen, das sich daraus ergibt. Der Zugriff auf die vollständige Übersicht aller relevanten Daten im Zusammenhang mit der Sozialauswahl muss streng restriktiv gehandhabt werden und ist im Idealfall allein der Leitung der Personalabteilung möglich.

Jana Thieme, Dipl.-Jur. Univ., ist Geschäftsführerin und Datenschutzexpertin der TH Datenschutz+ GmbH (info@th-datenschutz.plus).

Prüfpunkt	Erläuterung	OK
Benutzer		
Sind die Benutzerkonten von ausgeschiedenen Mitarbeitenden gelöscht?	Dies ist unter „Benutzer“ ⇨ „Gelöschte Benutzer“ einsehbar.	☐
Sind nur die erforderlichen Berechtigungen vergeben?	Dies ist durch Klicken auf den jeweiligen Benutzer einsehbar.	☐
Muss der Benutzer bei der ersten Anmeldung das Passwort ändern?	Dies ist beim Hinzufügen eines Benutzers einstellbar.	☐
Ist die Mehrfachauthentifizierung aktiv?	Dies ist durch Klicken auf den jeweiligen Benutzer und dann „Mehrstufige Authentifizierung verwalten“ einsehbar.	☐
Ist das Beweissicherungsverfahren deaktiviert?	Die Funktion sollte generell nur in bestimmten Fällen verwendet werden.	☐
Gruppen/Rollen		
Erfüllen/entsprechen die angelegten Gruppen bzw. zugeordneten Rollen dem Erforderlichkeitsprinzip?		☐
Sind freigegebene (Gruppen-)Postfächer nur erforderlichen Personen zugänglich?		☐

Exemplarische Checkliste für mögliche Prüfinhalte für Benutzer, Gruppen und Rollen. Abonnenten finden die Checkliste als Word-Datei unter https://ogy.de/cl-pruefung-rollen-ms365.

Das Admin Center

Prüfpflichten des DSB bei Microsoft 365 (Teil 3)

Im letzten Beitrag zu Microsoft 365 (MS 365) haben Sie erfahren, wie Sie den Compliance-Manager für Ihre Prüfungen verwenden, wenn MS 365 bereits vorhanden ist. Wie starten Sie jedoch, wenn Sie erst vor der Einführung von MS 365 stehen?

Für den Fall, dass Ihre Organisation oder Ihr Mandant erst plant, MS 365 einzuführen, sollten Sie das Admin Center kennen. Es bietet wichtige Konfigurationsmöglichkeiten zum Datenschutz. Zudem ist das Admin Center elementar für Ihre späteren Prüfungen.

Überblick über das Admin Center

Das Admin Center unterstützt Sie dabei, verschiedene Grundeinstellungen für MS 365 vorzunehmen. Hier geht es z.B. um die Verwaltung von

- **Benutzern** (Benutzer anlegen/löschen, Kennwort zurücksetzen, Lizenzen zuweisen, Rollen verwalten, Benutzer Gruppen zuweisen etc.),
- **Geräten** (Geräte verwalten, Überblick über durch Richtlinien geschützte Geräte, verlorene Geräte, Fernlöschung etc.),
- **Gruppen** (Gruppen anlegen, Mitglieder einsehen, Einstellungen vornehmen),
- **Rollen** (Rollenvergabe zur Wahrnehmung differenzierter Administrationsaufgaben in den Admin Centers),
- **Ressourcen** (Anlage von gemeinsam genutzten Ressourcen wie Konferenzräumen und Firmenfahrzeugen),
- **Abrechnungen und Lizenzen** (Auswahl der MS-365-Lizenzart, Produkte, Abrechnungsdetails),
- **Support** (Supportanfragen an MS) und
- **Einstellungen** (Grundeinstellungen für die Anwendungen vornehmen).

Datenschutzfreundliche Voreinstellungen für die Organisation

Als Datenschutzbeauftragte/r (DSB) müssen Sie sich die „Einstellungen“ ⇨ „Einstellungen der Organisation“ genauer anschauen. Hier nehmen Sie wichtige Grundeinstellungen vor bzw. empfehlen, diese Einstellungen vorzunehmen:

1. **Deaktivieren Sie nicht benötigte Dienste**. Unter „Dienste“ deaktivieren Sie die Anwendungen, die Ihre Organisation nicht zum Arbeiten benötigt. Das entspricht datenschutzfreundlichen Voreinstellungen (privacy by default).
2. Nehmen Sie **datenschutzfreundliche Voreinstellungen** für verbleibende Dienste vor. Unter „Sicherheit und Datenschutz“ wählen Sie Ihre Einstellungen aus. Zu prüfende Kriterien sind z.B.
   - die Einstellung zur „Datensammlung durch Bing“. Ist sie aktiv, sodass Bing Daten zur Suche in der Organisation erfassen darf, oder ist sie deaktiviert?
   - das Datenschutzprofil. Hier sollte ein Link zur Datenschutzrichtlinie Ihrer Organisation eingetragen und ein Ansprechpartner für den Datenschutz benannt sein.
   - die Kennwortablaufrichtlinie. Tragen Sie die Zeitdauer ein, ab wann Kennwörter ablaufen und von den Anwenderinnen und Anwendern zu ändern sind. Dieser Wert sollte den zentralen Passwortvorgaben entsprechen. Die Kriterien für Passwörter lassen sich hier übrigens nicht verändern.

– das Teilen von Inhalten. Unter „Teilen“ lässt sich konfigurieren, ob Benutzer neue Gäste zur Organisation hinzufügen dürfen. Im Sinne datenschutzfreundlicher Voreinstellungen sollte das standardmäßig deaktiviert sein.

Organisationsprofil: weitere Einstellungs- und Prüfmöglichkeiten

Im „Organisationsprofil“ können Sie unter „Datenresidenz“ die Datenmigration in ein deutsches Rechenzentrum anstoßen, wie in Teil 1 erwähnt. Ist nicht bekannt, wo die Daten Ihrer Organisation aktuell gespeichert sind, so lässt sich das unter „Datenspeicherort“ einsehen. Für einzelne Dienste erhalten Sie Hinweise, wo die ruhenden Daten aktuell gespeichert sind.

Abschließend bietet es sich unter „Releaseeinstellungen“ an, „Gezieltes Release für ausgewählte Benutzer“ zu wählen. Damit können bestimmte Anwender neue Funktionen prüfen, bevor die IT sie für die gesamte Organisation freigibt. Als weitere datenschutzfreundliche Einstellung sei „Integrierte Apps“ genannt. Dort können DSB prüfen, ob bzw. welche Apps von Dritten in MS 365 im Einsatz sind. Entdecken Sie hier Einträge, stellt sich die Frage nach dem Zweck der App, wer diese nutzt und welche Daten dabei verarbeitet und ggf. an Dritte übermittelt werden.

WICHTIG

Jeder DSB, dessen Organisation MS 365 einsetzt, sollte das Admin Center kennen, um datenschutzfreundliche Voreinstellungen zu prüfen. Da dieser Artikel nur einen Auszug der Möglichkeiten widerspiegelt, sehen Sie sich die weiteren Einstellungen zusätzlich an oder lassen Sie sie sich zeigen. So achten Sie bereits bei der Einführung von MS 365 auf datenschutzfreundliche Voreinstellungen bzw. berücksichtigen sie später bei Prüfungen.

Produktivitätsbewertung deaktivieren

Bei den Berichten finden gut informierte DSB Bekanntes, z.B. die Produktivitätsbewertung. Sie analysiert das Arbeitsverhalten des einzelnen Anwenders, erzeugt auf Basis aller Kolleginnen und Kollegen Durchschnittswerte und setzt das eigene Arbeitsverhalten in Relation dazu:

- Die Mitarbeitererfahrung vergleicht das eigene Verhalten in der Kommunikation, mit Meetings und in der Zusammenarbeit mit anderen sowie mit Dokumenten mit den Werten der Kollegen und Kolleginnen.
- Die Technologieerfahrung soll Hinweise darauf geben, wie die Anwender unterschiedliche Anwendungen nutzen.

Die Produktivitätsbewertung lässt sich unter den „Einstellungen der Organisation“ ⇨ „Dienste“ ⇨ „Produktivitätsbewertung“ aktivieren oder deaktivieren.

Berichte datenschutzfreundlich einrichten

Ein weiterer Punkt der Prüfpflichten ist der Bereich „Berichte“ ⇨ „Verwendung“. Hier finden Sie eine Vielzahl von Auswertungen, etwa über aktive Benutzer, Aktivitäten in Bezug auf E-Mails, MS Teams etc.

Zwar können nur Administratoren die Berichte einsehen. Doch lassen die Analysen Rückschlusse auf das Arbeitsverhalten einzelner Nutzer zu. So ist z.B. einsehbar, wie viele E-Mails jemand gesendet bzw. empfangen hat oder an wie vielen Besprechungen jemand teilgenommen hat. Speziell für Yammer, als soziales Netzwerk des Unternehmens, können Sie erkennen, welcher Benutzer wie aktiv war. Denkbar wäre dann, bestimmten Mitarbeitenden eine Minderleistung zu unterstellen.

Den Personenbezug in den Berichten entfernen Sie ebenfalls unter „Einstellungen der Organisation“ ⇨ „Dienste“ ⇨ „Produktivitätsbewertung“. Fordern Sie auch diese Einstellung als Standardeinstellung ein.

Julian Häcker, Geschäftsführer der ENSECUR GmbH, löst als Datenschutzberater seit 2010 die Praxisherausforderungen im Datenschutzalltag von Organisationen.

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, 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.:
09100-4088

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.

Datensicherung

Am falschen Ende gespart

Eine sorgfältige Datensicherung ist unverzichtbar und ohne Alternative. Aber Datensicherung muss auch funktionieren. Dazu gehört u.a. die Erkenntnis, dass alles, was gut funktionieren soll, Geld kostet. Hier am falschen Ende zu sparen, kann sehr teuer werden und großen Aufwand verursachen.

Eine Arztpraxis wollte alles besonders gut machen. Man hatte einen eigenen Server und sicherte jeden Abend die Daten auf ein Magnetband. Dazu musste eine Mitarbeiterin das Speichergerät an den Server anstecken, das Datenband einlegen, auf „Ready" warten und dann den Speicherknopf drücken. Erst wenn die grüne LED aufleuchtete, ging es für die Mitarbeiterin nach Hause.

Die alte Festplatte geht in den Ruhestand

Eines Tages verabschiedete sich die sieben Jahre alte Festplatte des Systems „in den Ruhestand". Sie war kaputt. Aber genau für solche Fälle hat man ja die Datensicherung. Also schnell die neue Festplatte einsetzen und die Rücksicherung starten. So weit die Theorie.

Ein Verkaufstrick?

Die Praxis sah leider anders aus: Speicherband eingeschoben – es tat sich nichts. Der Grund war so einfach wie fatal: Das Band war so oft für die Datensicherung benutzt worden, dass die magnetische Beschichtung mittlerweile komplett abgeschmirgelt war.

Schuld war die Sparsamkeit des Chefs. Ein Speicherband kostet 80 € und sollte eigentlich nicht länger als sechs Monate im Einsatz sein. Das erschien dem Chef zu teuer. „Die halten sicher länger, das ist ein Verkaufstrick!", so seine Überzeugung. Und so beschaffte er nur zwei Bänder. Vor drei Jahren. Immerhin funktionierte die zweite Bandsicherung tatsächlich noch – doch sie war sechs Wochen alt.

Teure Sparsamkeit

Die Folgen: Weil er keine Einzelnachweise bei den Kassenpatientinnen und -patienten hatte, bekam er von der Kassenärztlichen Vereinigung einen ziemlich hohen Abzug. Von den Privatpatienten existierten zwar noch Papierunterlagen. Aber all diese Informationen für die Rechnungen nachzutragen, dauerte insgesamt 30 Personentage. Und kostete entsprechend viel Geld.

Der finanzielle Ausfall für die Praxis lag für die zwei betroffenen Quartale bei ca. 40.000 €. Dafür hätte der Chef so einige Speicherbänder bekommen.

Eberhard Häcker ist seit vielen Jahren selbstständig mit Schwerpunkt Datenschutzberatung. Als externer DSB weiß er: „Es gibt nichts, was es nicht gibt."

IN DER NÄCHSTEN AUSGABE

Arbeitsorganisation für DSB in 4 Schritten

Diese Prozesse und Tools helfen Ihnen, typische Arbeitsabläufe zu vereinfachen.

360-Grad-Feedback

So bekommen Sie diese Methode, Arbeitsleistung und Verhalten zu bewerten, aus Datenschutzsicht in den Griff.

Geldbußen nach der DSGVO

Das eine Gericht reduziert eine Geldbuße erheblich, das andere kassiert sie gleich ganz. Wie ist das einzusortieren?