www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT | Februar 2021

Bild: iStock.com/Melpomenem

Das richtige Verhalten gegenüber der Aufsichtsbehörde kann dazu beitragen, eine Geldbuße abzuwenden oder zumindest gering zu halten

Das können DSB raten

Dos and Don'ts im datenschutzrechtlichen Bußgeldverfahren

Bußgelder vermeiden? Das ist sicherlich am besten, geht aber in der Praxis realistisch betrachtet nicht immer. Was also tun, wenn das Kind in den Brunnen gefallen ist? Und was lassen Verantwortliche lieber bleiben? To do or not to do? Hier die Antworten.

Der Mensch ist einfach gestrickt. Droht ihm eine Geldstrafe oder ein Bußgeld, so wird er stets versuchen, nach Möglichkeit nicht zahlen zu müssen oder, wenn sich dies nicht vermeiden lässt, möglichst wenig zu zahlen.

Angesichts der horrenden Bußgelder, die nach der Datenschutz-Grundverordnung (DSGVO) möglich sind, ist das auch nur allzu verständlich. Schließlich können diese Geldbußen bis zu 20 Millionen Euro betragen oder im Extremfall bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens. Art. 83 DGSVO legt dabei ausdrücklich fest, dass die Verhängung von Geldbußen aufgrund von Verstößen gegen diese Verordnung „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein muss.

Abschreckung in zwei Richtungen

Bußgelder sollen v.a. eines: abschrecken. Und zwar deshalb, damit sich Verstöße gegen datenschutzrechtliche Vorschriften möglichst nicht wiederholen. Abschreckung funktioniert dabei in zwei verschiedene Richtungen:

- Zum einen richtet sie sich gegen den Täter. Eine spürbare Sanktion soll ihn davon abhalten, so weiterzumachen wie bisher.
- Zum anderen tragen hohe Bußgelder dazu bei, andere davon abzuschrecken, in gleicher Weise datenschutzrechtlich nachlässig zu agieren.

Im Juristendeutsch nennt man diese beiden Zielrichtungen Spezial- und Generalprävention. →

Editorial

Ricarda Veidt, Chefredakteurin

Sagen Sie uns Ihre Meinung!

Liebe Leserin, lieber Leser! Sie sind hoffentlich gesund und erholt ins neue Jahr gestartet.

Über die Feiertage ist auch ein runderneuerter Internetauftritt der Datenschutz PRAXIS an den Start gegangen. Sie finden ihn wie gewohnt unter www.datenschutz-praxis.de. Abonnenten der Zeitschrift können sich nun oben rechts über den Button „Mein DP" anmelden, um auf die Abo-Inhalte und das Ausgaben-Archiv, das Sie unter „Zeitschrift" finden, zuzugreifen.

Wir werden den Auftritt in der nächsten Zeit noch weiterentwickeln, sodass Ihnen bald zusätzliche Funktionen wie Umfragen und Toolsammlungen zur Verfügung stehen.

Geben Sie uns gern Rückmeldung, wie Ihnen der neue Auftritt gefällt, wie Sie sich zurechtfinden, was Ihnen fehlt und was wir besser machen können. Schreiben Sie mir einfach an ricarda.veidt@weka.de. Ich freue mich sehr, von Ihnen zu lesen. Denn nur mit Ihren Anregungen aus der Praxis können wir die Seite weiter für Sie optimieren.

Bleiben Sie gesund!
Ihre Ricarda Veidt

Was tun, damit es bei einem „blauen Auge" bleibt?

Der allerbeste Umgang mit Bußgeldverfahren ist sicherlich der, ein solches generell zu vermeiden. Mit anderen Worten: möglichst alle datenschutzrechtlichen Bestimmungen einzuhalten. Gelingt das nicht und kommt es zu einem Bußgeldverfahren, so ist es wichtig zu wissen, was es einerseits unbedingt zu vermeiden gilt und was Verantwortliche andererseits unbedingt tun sollten, damit das eigene Unternehmen oder gegebenenfalls die eigene Person, wenn sie für den Verstoß verantwortlich gemacht wird, mit höchstens einem blauen Auge davon kommt.

Raten Sie als Datenschutzbeauftragte(r) (DSB) Ihrem Unternehmen bzw. Ihren Mandaten dazu, sich möglichst an die folgenden Regeln zu halten.

DON'T: Stecken Sie den Kopf nicht in den Sand!

Unser ehemaliger Bundeskanzler Helmut Kohl hat es zwar vielfach erfolgreich vorgemacht: Gibt es ein Problem, einfach aussitzen. Das ist im datenschutzrechtlichen Bußgeldverfahren jedoch auf jeden Fall der falsche Weg. Anders als etwa in einem straßenverkehrsrechtlichen Bußgeldverfahren empfiehlt es sich im Datenschutzbereich auf jeden Fall, so frühzeitig wie möglich aktiv zu werden. Das kann sogar so weit gehen, aktiv mit einer Selbstanzeige dazu beizutragen, dass die Aufsichtsbehörde Kenntnis von dem Verstoß erhält und ein Verfahren einleitet.

So gut kooperieren wie irgend möglich

Warum das? Bei Verstößen gegen die Straßenverkehrsordnung (StVO) geht es nur um vergleichsweise niedrige Bußgelder. Hier wirken sich taktische Fehler nicht allzu schlimm aus. Das ist bei datenschutzrechtlichen Verstößen nicht der Fall.

Zudem kann zwar im Straßenverkehr Schweigen v.a. dann sinnvoll sein, wenn man nicht selbst gefahren ist und einen Anhörungsbogen nur als Halter eines Fahrzeugs erhalten hat. Bei datenschutzrechtlichen Verstößen sollten Verantwortliche dagegen auf jeden Fall all ihre Chancen nutzen, die Datenschutzaufsichtsbehörde soweit irgend möglich im positiven Sinne zu beeinflussen.

Das hat v.a. folgenden Hintergrund: Nach Art. 83 Abs. 2 DSGVO steht der Aufsichtsbehörde ein Ermessen zu, ob sie überhaupt ein Bußgeld verhängen will oder ob ihr nicht im konkreten Einzelfall mildere Mittel zur Verfügung stehen, die aus ihrer Sicht ausreichend sind. Dabei handelt es sich im mildesten Fall um bloße Hinweise.

PRAXIS-TIPP

Besteht die Chance, dass sich die Datenschutzaufsichtsbehörde mit milden Maßnahmen begnügt, sollten Verantwortliche unbedingt einen kooperativen Weg beschreiten. Gerade in den Fällen, in denen ein Verantwortlicher selbst einen Verstoß angezeigt hat, halte ich diesen Weg für den besten, um zu erreichen, dass die Aufsicht gar kein Bußgeld verhängt. Je frühzeitiger ein Unternehmen bei erkanntem Verstoß die Aufsichtsbehörde informiert, umso eher lassen sich mögliche schwerwiegende Folgen vermeiden. Trifft man sich erstmal vor Gericht, so ist es ungleich schwieriger, eine milde Rechtsfolge zu erreichen.

Möglich sind auch Verwarnungen oder z.B. Teiluntersagung bestimmter Datenverarbeitungsvorgänge.

Selbst wenn sich die Behörde nicht davon abbringen lässt, einen Bußgeldbescheid zu erlassen, können Verantwortliche sich bemühen, alles zu tun, was zu einem möglichst niedrigen Bußgeld beiträgt. Dazu ist freilich wichtig, zu wissen, welche Faktoren die Höhe des Bußgelds bestimmen und wie sich diese ggf. beeinflussen lassen. Daraus ergeben sich für Unternehmen die im Folgenden vorgestellten weiteren „Dos" und „Don'ts".

DO: Schalten Sie frühzeitig einen kompetenten Rechtsanwalt ein!

Dieser Rechtsanwalt sollte sich idealerweise sowohl im Datenschutzrecht als auch im Bußgeldverfahren auskennen. Das kann v.a. deswegen sehr wichtig sein, weil es im Bereich des Datenschutzes nicht nur Ordnungswidrigkeiten gibt, sondern auch Straftaten. Jedes Bußgeldverfahren lässt sich nämlich auch leicht in ein Strafverfahren überführen.

Je schwerwiegender sich ein Verstoß darstellt, umso wichtiger ist es, einen Rechtsanwalt zu beauftragen. Wichtig ist auch, dass Unternehmensleitung, Datenschutzbeauftragte(r) und Verteidiger sich möglichst eng abstimmen und alle zentralen Informationen austauschen.

Zwar kosten Rechtsanwälte Geld. Das kann sich aber v.a. bei sehr komplizierten Sachverhalten angesichts der schon erwähnten immensen Höhe von Bußgeldern schnell bezahlt machen. Ein kompetenter Anwalt wird in aller Regel mögliche Fehlerquellen erkennen, sie ausschließen und alles tun, was in der gegebenen Situation sinnvoll ist.

DO: Geben Sie eine Stellungnahme ab!

Wie eingangs erwähnt gilt im straf- und bußgeldrechtlichen Bereich zwar häufig der Grundsatz „Reden ist Silber, Schweigen ist Gold." Gerade aber, wenn das Gesetz Möglichkeiten vorsieht, durch aktives Tun die Aufsichtsbehörde gnädig zu stimmen, kann Schweigen kontraproduktiv sein. Raten Sie als DSB daher dazu, die folgenden Dinge zu beherzigen:

DO: Nehmen Sie Akteneinsicht!

Richtig verteidigen kann sich nur, wer die Akten kennt. § 49 Gesetz über Ordnungswidrigkeiten (OWiG) gewährt Ihnen auf Antrag – also nicht automatisch – Einsicht in die Akten, soweit das den Untersuchungszweck nicht gefährdet und keine überwiegenden schutzwürdigen Interessen Dritter entgegenstehen.

Beauftragen Sie möglichst einen Rechtsanwalt damit, für Sie Akteneinsicht zu nehmen und eine vernünftige Verteidigungsstrategie im Sinne der nachfolgenden Dos und Don'ts zu entwickeln.

DO: Gehen Sie nur auf Dinge ein, die sich für Sie positiv auswirken können & DON'T: Schreiben Sie nichts zu Dingen, auf die es nicht ankommt!

Bei diesen Tipps geht es nicht darum, die Aufsichtsbehörde nicht zu langweilen. Ziel ist, nicht auf Dinge hinzuweisen, die nachteilig sind, und zudem nicht den Blick auf Aspekte zu verstellen, die fürs Unternehmen günstig sind.

So ist es in aller Regel müßig, auf Art, Schwere und Dauer eines datenschutzrechtlichen Verstoßes vertieft einzugehen. Art und Dauer eines datenschutzrechtlichen Verstoßes stehen meist ohnehin fest. Die Schwere richtet sich u.a. nach einzelnen Gesichtspunkten, beispielweise wie viele Personen von dem Verstoß betroffen sind – nur einer, eine bestimmte Personengruppe oder gar alle Kunden eines Unternehmens – und um welche Art von Daten es geht – Adressdaten, Kontodaten oder z.B. Gesundheitsdaten.

Auch diese Aspekte lassen sich nicht beeinflussen. Es schadet allerdings nicht, darauf hinzuweisen, dass von einem Verstoß nur wenige Personen betroffen sind und keine sensiblen Daten im Spiel sind.

DO: Gehen Sie auf das Verschulden ein!

Vorsatz und Fahrlässigkeit sind zwei völlig unterschiedliche Schuldformen. Vorsätzliches Verhalten wird immer strenger geahndet als fahrlässiges Handeln. So einfach wie es der Laie sieht, der häufig Vorsatz mit Absicht gleichsetzt, ist die Abgrenzung juristisch gesehen allerdings leider nicht. Sie kann im Einzelfall sehr schwierig sein, denn Vorsatz ist schon dann gegeben, wenn man die mögliche Folge eines Verstoßes „billigend in Kauf nimmt".

Hingegen liegt bewusste Fahrlässigkeit vor, wenn jemand die negativen Folgen zwar sieht, aber hofft, dass sie nicht eintreten. Man kann hier z.B. an das bewusste Bestehenlassen einer Sicherheitslücke denken, die, wenn sie von Hackern ausgenutzt wird, zu Datendiebstahl und Schäden bei den Betroffenen führen kann.

Die beiden Schuldformen Vorsatz und Fahrlässigkeit lassen sich mit folgender Faustformel voneinander abgrenzen:

- Vorsatz liegt vor, wenn der Verantwortliche in Bezug auf die Folgen denkt: „Na, wenn schon."
- Hingegen ist Fahrlässigkeit gegeben, wenn er sich sagt: „Wird schon gut gehen."

Daraus ergibt sich grundsätzlich die Chance, das eigene Handeln nur als fahrlässig erscheinen zu lassen. Freilich muss der Verantwortliche dies schlüssig, plausibel und glaubhaft darstellen. Eine entsprechende Einlassung wird die Datenschutzaufsichtsbehörde in aller Regel glauben, jedenfalls aber nicht ohne Weiteres widerlegen können. Denn wer kann schon in die Köpfe sehen?

Vorsicht ist hier allerdings in jedem Fall geboten, denn die Einlassung zur Fahrlässigkeit muss zur Gesamtsituation passen. Und wenn es Beweismittel gibt, die Vorsatz nahelegen, könnte der Schuss →

nach hinten losgehen und das Bußgeld deutlich höher ausfallen als ursprünglich erwartet.

DO: Tun Sie alles, um Schaden zu mindern!

Das ist im datenschutzrechtlichen Bereich nicht immer so einfach wie etwa bei einer einfachen Körperverletzung, bei der man dem Opfer ein Schmerzensgeld zahlen kann. Sind sensible Daten erst einmal in falsche Hände geraten, so lässt sich der Schaden nicht immer beziffern. Ist dies aber der Fall, z.B. bei einem verschuldeten Datenklau, der zu unberechtigten Abhebungen von Konten der Betroffenen geführt hat, so sollten Verantwortliche einen solchen Schaden so schnell wie möglich und vollständig begleichen.

Die Aufsichtsbehörde ist nach Art. 83 Abs. 2 Buchst. c DSGVO gehalten, die Schadenswiedergutmachung zu berücksichtigen, wenn sie die Schwere des Datenschutzverstoßes einordnet.

DON'T: Gehen Sie nicht auf frühere Verstöße ein!

Vielleicht hat Ihr Unternehmen oder Mandant Glück und diese früheren Verstöße sind aus datenschutzrechtlichen Gründen nicht mehr gespeichert. Oder sie sind der Aufsichtsbehörde aus anderen Gründen nicht bekannt, weil die Verstöße etwa in einem anderen Bundesland stattgefunden haben.

Weiß die Aufsichtsbehörde von früheren Verstößen, so wird sie diese ohnehin berücksichtigen. Sie muss es sogar. Sind Sie der Aufsichtsbehörde aber nicht bekannt, haben Sie schlichtweg Glück gehabt. Nicht schaden kann freilich der zutreffende Hinweis, dass man sich bislang nie etwas zuschulden hat kommen lassen.

DO: Helfen Sie, so gut es geht, bei der Aufklärung mit!

Der Umfang der Zusammenarbeit mit der Aufsichtsbehörde ist ebenfalls ein Kriterium, das Bußgeld geringer ausfallen zu lassen. Außerdem ist es häufig im Unternehmensinteresse, wenn die konstruktive Zusammenarbeit Schwachstellen entdeckt und beseitigt. Das vermeidet künftige Datenschutzverstöße.

PRAXIS-TIPP

In manchen Fällen werden Verantwortliche gar nicht wissen, wie es zu dem Verstoß, beispielsweise einem Datenverlust aufgrund vermeidbarer Sicherheitslücken, gekommen ist. Dann ist es besonders sinnvoll, konstruktiv mit der Aufsichtsbehörde zusammenzuarbeiten und ihren Sachverstand zu nutzen.

DO: Versäumen Sie keine Fristen!

Ist ein Bußgeldbescheid ergangen, den der Verantwortliche nicht akzeptieren kann, so muss er einen Einspruch innerhalb von zwei Wochen nach Zustellung entweder schriftlich oder zur Niederschrift der Aufsichtsbehörde einlegen. Ist ein Verteidiger beauftragt, so wird er sich darum kümmern, Fristen und Formvorschriften einzuhalten.

Beachtet man diese Regeln nicht, so wird das Gericht den Einspruch als unzulässig verwerfen. Hiergegen lässt sich dann zwar sofortige Beschwerde einlegen. Sie wird aber in der Regel erfolglos bleiben, wenn der Verantwortliche die Frist schuldhaft versäumt hat.

Wer unverschuldet eine Frist versäumt, der kann unverzüglich Wiedereinsetzung in den vorigen Stand beantragen. Ist das fehlende Verschulden glaubhaft, so stehen die Chancen gut, dass sich die Fristversäumnis nicht auswirkt. Wichtig ist, zugleich mit dem Wiedereinsetzungsantrag den versäumten Einspruch einzulegen. Entsprechendes gilt für die Einlegung einer Rechtsbeschwerde, wenn man mit dem Urteil nicht zufrieden ist.

Dos & Don'ts vor Gericht

Im gerichtlichen Verfahren empfiehlt sich das folgende Vorgehen:

DO: Benennen Sie frühzeitig vor einer Verhandlung Beweismittel, die zu einer günstigen Beurteilung durch das Gericht führen können!

Hat der Verantwortliche das nicht schon im Verfahren vor der Aufsichtsbehörde gemacht, sollte er dem Gericht die Chance geben, dass es bei seiner Entscheidung die für ihn günstigen Aspekte erkennen und berücksichtigen kann.

DO: Kommen Sie in jedem Fall persönlich zur Hauptverhandlung und machen Sie einen möglichst guten Eindruck!

Natürlich kann man sich im Bußgeldverfahren auch von seinem Verteidiger vertreten lassen. Aber einen guten Eindruck können Sie nur machen, wenn Sie selbst erscheinen. Es mag ja banal klingen – aber es hilft, wenn man sich ordentlich anzieht. Der Grundsatz „Kleider machen Leute" hat durchaus auch heute noch seine Berechtigung. Sie zeigen nämlich auch dadurch Ihre Achtung vor dem Gericht.

Stehen Sie auf, wenn das Gericht den Saal betritt und unterbrechen Sie den Vorsitzenden nicht. Warten Sie, bis Ihnen das Wort erteilt wird. Bleiben Sie stets sachlich und halten Sie sich an die Absprachen mit Ihrem Verteidiger.

Und für die Zukunft gilt:

DO: Befolgen Sie künftig alle Anforderungen der DSGVO!

Ein kompetenter Datenschutzbeauftragter oder eine ebensolche Datenschutzbeauftragte, sinnvoll in die Organisationsstruktur eingebaut und rechtzeitig bei allen relevanten Fragen einbezogen, ist ein wichtiger Faktor, um Datenschutzverstöße zukünftig zu vermeiden. Verantwortliche sollten zudem keine Investitionen in die Datensicherheit scheuen. Sie zahlen sich schnell aus.

Dr. Claus Pätzel ist Vorsitzender Richter am Oberlandesgericht München. Zuvor leitete er die Strafabteilung des Landgerichts Augsburg.

Bild: iStock.com/Prostock-Studio

Die (gemeinsame) Verantwortlichkeit, die Frage der Einwilligung und die Transparenzvorschriften sind die drei wesentlichen Problemkreise beim datenschutzkonformen Social-Media-Marketing

Datengetriebene Werbung

Was geht datenschutzkonform im Social-Media-Marketing?

Marketing im Digitalzeitalter ist eine hochkomplexe Angelegenheit. Damit der Datenschutz dabei nicht auf der Strecke bleibt, sensibilisieren Sie die Marketingverantwortlichen dafür, was möglich ist.

Soziale Netzwerke sind für einen Großteil der Internetnutzer nicht mehr wegzudenken. Angesichts der Tatsache, dass z.B. 65 % der 14- bis 29-jährigen Deutschen mindestens einmal wöchentlich Instagram nutzen, ist diese Form des Marketings vielfach besonders erfolgversprechend.

Gerade soziale Netzwerke bieten immer raffiniertere Funktionen, um werbende Unternehmen und Kunden zusammenzuführen. Gleichzeitig drängen Marketingabteilungen und -agenturen die Verantwortlichen, von neuen Marketingfunktionen möglichst schnell und umfangreich Gebrauch zu machen.

Aus datenschutzrechtlicher Sicht lässt sich das Social-Media-Marketing dagegen nicht nur mit Begeisterung sehen. Insbesondere weil die Plattformbetreiber bei dieser Form des Onlinemarketings eine unüberschaubare Vielzahl an personenbezogenen Daten verarbeiten, ist Vorsicht geboten. Dabei hilft es nicht, dass die US-Anbieter in Sachen „Transparenz der Datenverarbeitung“ häufig sehr zu wünschen übriglassen.

Dieser Beitrag gibt einen Überblick über aktuelle Fragen rund um das Social-Media-Marketing aus datenschutzrechtlicher Sicht und zeigt Handlungsmöglichkeiten für Unternehmen auf.

Die datenschutzrechtliche Eingangstür: Verantwortlichkeit für die Datenverarbeitung

Reichweite einer Mitverantwortung des Unternehmens

Social-Media-Marketing wird für werbende Unternehmen erst dann datenschutzrechtlich relevant, wenn sie bei der Ausführung (mit-)verantwortlich für die Datenverarbeitung nach Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO) sind. Nur soweit das Unternehmen auch Verantwortlicher ist, muss es für die Einhaltung der datenschutzrechtlichen Vorgaben sorgen.

Zum Themenbereich des Social-Media-Marketings hat der Europäische Gerichtshof (EuGH) in den vergangenen Jahren zwei Urteile gefällt, die zumindest für zwei Teilbereiche von Facebook eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO bestätigten:

- Bei Facebook-Fanpages (5.6.2018 – C-210/16, Urteil ist abrufbar unter https://ogy.de/EuGH-Fanpages) hat der EuGH eine gemeinsame Verantwortlichkeit aufgrund der sogenannten „Seiten-Insights“-Funktionen angenommen. Sie erlauben dem Fanpage-Betreiber, Nutzeraktionen zu parametrisieren und auszuwerten, um die Fanpage und die Werbeanzeigen zielgruppenoptimiert zu gestalten.
- Bei der Entscheidung „Fashion ID“ (29.7.2019 – C-40/17, abrufbar unter https://ogy.de/EuGH-FashionID) nahm der Europäische Gerichtshof eine gemeinsame Verantwortlichkeit bei der Einbindung des „Facebook-Like-Buttons“ auf der eigenen Website an. In dieser Entscheidung ging der EuGH jedoch erstmals auch differenzierter auf die Reichweite der gemeinsamen Verantwortlichkeit ein und beschränkte sie auf die websitegebundene Datenerhebung und die anschließende Übermittlung an Facebook. →

Bloße Teilnahme = Mitverantwortung?

Einige deutsche Aufsichtsbehörden leiten demgegenüber bereits aus der bloßen Teilnahme an einem sozialen Netzwerk eine Mitverantwortung des Unternehmens ab, und zwar für die gesamte Verarbeitung der Kundendaten durch das soziale Netzwerk. Die sich infolgedessen für Unternehmen ergebenden Datenschutzpflichten, insbesondere die Informationspflichten, sind in der Praxis unerfüllbar.

Aufgrund der EuGH-Rechtsprechung ist jedoch zumindest zweifelhaft, ob ein derartig weites Verständnis der Reichweite der gemeinsamen Verantwortlichkeit einer gerichtlichen Prüfung standhält:

- Dagegen spricht, dass es in beiden zitierten Entscheidungen gerade nicht ausreichend war, dass das betroffene Unternehmen Facebook allein die Möglichkeit der Datensammlung eröffnet hat.
- Hinzukommen musste in beiden Fällen eine konkretere Einflussnahme auf die Mittel der Verarbeitung.
- Außerdem mussten sich zumindest gegenseitig ergänzende wirtschaftliche Zwecke vorhanden sein.

Targeting = Mitverantwortung?

Demgegenüber begründet das Targeting von Nutzern sozialer Netzwerke zum Zweck der zielgenauen Werbeansprache nach Ansicht der Aufsichtsbehörden in den meisten Fällen eine gemeinsame Verantwortlichkeit. Das bestätigte der Europäische Datenschutzausschuss (EDSA) in seinen im September 2020 veröffentlichten „Guidelines 08/2020 on the targeting of social media users“ (abrufbar unter https://ogy.de/edsa-targeting).

Jedoch kann auch beim Targeting die Reichweite der gemeinsamen Verantwortlichkeit nicht grenzenlos sein. Um eine Einzelfallbewertung kommt man bei der Durchführung von Social-Media-Marketing also nicht herum. Am Ende wird es aufgrund bestehender Unklarheiten häufig auf risikobasierte Entscheidungen hinauslaufen.

Der Rahmen für datengetriebenes Marketing

Was geht nun datenschutzrechtlich beim Social-Media-Marketing? In den meisten Fällen ist das abhängig von einer individuellen Risikobewertung. Unserer Ansicht nach lassen sich die Marketingaktivitäten in zwei Risikokategorien einteilen. Dabei lassen sich für beide Kategorien die Risiken reduzieren.

1. Geringes Risiko

Ein geringes Risiko stellt die bloße Teilnahme an einem sozialen Netzwerk mit standardmäßigen Aktivitäten wie dem Posten von Beiträgen oder Fotos dar. Das gilt so lange, wie der Verantwortliche keine Funktionen nutzt – wie z.B. die „Seiten-In-

Datenübermittlung in die USA

Schrems II: Das Aus für Social Media?

Mit seiner „Schrems-II“-Entscheidung (16.7.2020 – C-311/18, abrufbar unter https://ogy.de/EuGH-SchremsII; siehe auch Ehmann in Datenschutz PRAXIS 09/2020, Seite 1–4) hat der EuGH den Datentransfer in die USA auf Basis des Privacy Shield untersagt. Das bleibt nicht ohne Folgen für die sozialen Netzwerke.

Quasi alle relevanten sozialen Netzwerke (Facebook, Instagram, Twitter, YouTube) haben den Hauptsitz der Muttergesellschaft in den USA. Sie räumen sich über ihre Nutzungsbedingungen auch das Recht ein, Daten in die USA zu übertragen. Fallen diese Datentransfers in die gemeinsame Verantwortlichkeit des Unternehmens, müsste das Unternehmen nach Art. 44 ff. DSGVO dafür sorgen, dass das europäische Datenschutzniveau bei der Übertragung gewahrt wird. Das wird derzeit nicht rechtssicher gelingen.

Man kann allerdings argumentieren, dass das Unternehmen gar nicht (mit-) verantwortlich für den Datentransfer ist. Der EuGH hat insbesondere in der „Fashion-ID“-Entscheidung klargestellt, dass der Nutzer der Social-Media-Funktionen nur für die Vorgänge verantwortlich sein soll, für die er tatsächlich über die Zwecke und Mittel (mit)entscheidet.

Nun entscheidet z.B. der Website-Betreiber, der einen „Like-Button“ einbindet, zwar, dass die Daten zu Facebook Ireland (also dem Dienstanbieter) gehen. Ob und unter welchen Umständen diese Daten von Facebook Ireland allerdings in die USA gehen, entzieht sich dem Entscheidungsradius des Website-Betreibers.

Bild: iStock.com/VioletaStoimenova

sights“ bei Facebook-Fanpages –, die eine gemeinsame Verantwortlichkeit begründen. Selbst wenn einige Aufsichtsbehörden schon hier eine Mitverantwortung sehen, lässt sich das mit guten Argumenten auch ablehnen.

2. Erhöhtes Risiko

Ein erhöhtes Risiko stellt sich dann ein, wenn sich eine gemeinsame Verantwortlichkeit annehmen lässt. Zwar bietet Facebook für die zwei Fälle der Mitverantwortung, die der EuGH entschieden hat, entsprechende Vereinbarungen an. Nach Auffassung der deutschen Aufsichtsbehörden genügen diese aber den rechtlichen Anforderungen bislang nicht.

Noch höher ist das Risiko in den Fällen, in denen die Netzwerkbetreiber trotz gemeinsamer Verantwortlichkeit gar keine Vereinbarungen anbieten. Folgt man dem Europäischen Datenschutzausschuss, besteht dieses Problem in fast allen Fällen, in denen Unternehmen die Werbefunktionen sozialer Netzwerke nutzen.

Aktuell bleibt werbenden Unternehmen hier nur, bei den Netzwerken auf den Abschluss einer solchen Vereinbarung zu drängen und die Bemühungen zu dokumentieren – oder ganz auf das Marketing zu verzichten.

Zu beachten ist auch der Sonderfall des Tools „Custom Audience mit Kundenliste“ von Facebook. Es war bereits Gegenstand gerichtlicher Verfahren: Das Verwaltungsgericht Bayreuth und der Verwaltungsgerichtshof Bayern befassten sich im Jahr 2018 mit dem Tool. Im Ergebnis lehnten die Gerichte die von Facebook angenommene Auftragsverarbeitung ab und forderten als Rechtsgrundlage eine Einwilligung der Betroffenen. Eine Vereinbarung zur gemeinsamen Verantwortlichkeit bietet Facebook auch hier bislang nicht an.

Maßnahmen, um das Risiko zu reduzieren

Es gibt einige „Basics“, die Unternehmen in jedem Fall umsetzen müssen: Eine Datenschutzerklärung, sichtbar in das Social-Media-Profil eingebunden, stellt Transparenz über die Nutzung des Netzwerks her. Wichtig ist auch, auf bestehende Vereinbarungen über die gemeinsame Verantwortlichkeit hinzuweisen, etwa per Link auf die „Seiten-Insights-Ergänzung“ oder den „Zusatz für Verantwortliche“ von Facebook. Das verlangt Art. 26 Abs. 2 Satz 2 DSGVO.

Immer wenn Unternehmen Daten auf der eigenen Website erfassen oder Daten über Funktionen wie die „Custom Audience mit Kundenliste“ an die Netzwerke senden, sollten sie zudem eine wirksame Einwilligung der betroffenen Personen einholen. Wir empfehlen, eine Einwilligung auch bei der Einbindung von Technologien wie Pixeln oder Plug-ins einzuholen – selbst wenn die „Planet-49“-Entscheidung des BGH bislang nur für Cookies zu Werbezwecken geklärt hat, dass der Website-Betreiber eine Einwilligung einholen muss. Das deckt sich mit den Empfehlungen des EDSA aus seinen Guidelines 08/2020.

PRAXIS-TIPP

Empfehlenswert ist auch, die Best-Practice-Modelle für Social Media aus Baden-Württemberg (https://ogy.de/bw-soziale-netzwerke) und Rheinland-Pfalz (https://ogy.de/handlungsrahmen-soziale-medien) umzusetzen. Die Social-Media-Konzepte mit Risikoabschätzung und Sensibilisierung der Nutzer sind zwar primär für öffentliche Stellen gedacht – viele Punkte sind aber ebenso für Unternehmen zur Risikominimierung ratsam. Durch diesen Mehraufwand können Unternehmen gegenüber den Aufsichtsbehörden nachweisen, dass sie sich intensiv mit den Chancen und Risiken des Social-Media-Marketings auseinandergesetzt haben und den Datenschutz dabei im Blick behalten.

Fazit: Drei wesentliche Problemkreise

Social-Media-Marketing ist eine komplexe Angelegenheit. Das macht die datenschutzrechtliche Bewertung nicht einfach. Das Thema lässt sich dabei jedoch auf drei wesentliche Problemkreise eingrenzen:

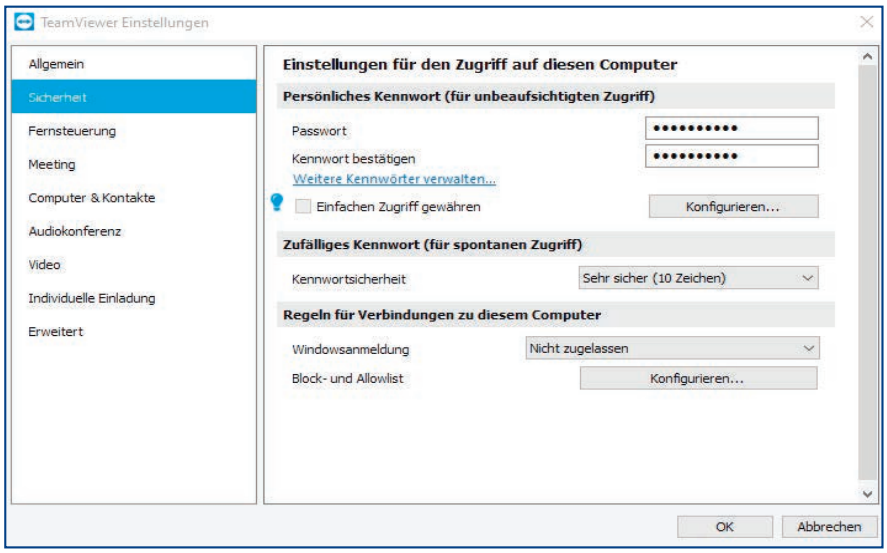
1. die (gemeinsame) Verantwortlichkeit,
2. die Frage der Einwilligung und
3. die Einhaltung von Transparenzvorschriften.

Im Hinblick auf die gemeinsame Verantwortlichkeit gilt es, genau zu prüfen, ob eine solche vorliegt. Hierbei sind insbesondere die differenzierten Maßstäbe des EuGH aus dem „Fashion-ID“-Verfahren heranzuziehen. Das Papier des EDSA aus dem September kann eine zusätzliche Richtschnur geben.

Schwierig ist der Umgang mit Fällen, in denen die Netzwerkbetreiber keine entsprechenden Vereinbarungen anbieten. Der LfDI Baden-Württemberg verabschiedete sich Anfang 2020 mangels Vereinbarung per „Twexit“ von Twitter und forderte alle Behörden auf, es ihm gleichzutun. Aufgrund kräftigen Gegenwinds ist er mittlerweile zurückgerudert und hat Guidelines für die Nutzung sozialer Netzwerke veröffentlicht. Das können auch betroffene Unternehmen als gewisse Kompromissbereitschaft der Behörden werten. Nichtsdestoweniger bleibt für Unternehmen leider eine teils ungewisse Situation.

In Bezug auf die Einwilligung sollten Verantwortliche insbesondere die Vorgaben des EuGH und des BGH aus der Rechtssache „Planet 49“ beachten. Das gilt sowohl für die Datenerfassung auf der Website als auch für die davon unabhängige Weitergabe von Kundendaten. Letztlich sollten Verantwortliche die Prozesse in jedem Fall durch entsprechende Datenschutzhinweise bestmöglich transparent machen – dabei reichen den Behörden pauschale Beschreibungen wie „Werbung“ für Targeting-Aktivitäten nicht aus.


Dr. André Schmidt (schmidt@lutzabel.com) und Niklas Vogt (vogt@lutzabel.com) sind Rechtsanwälte der Wirtschaftskanzlei LUTZ | ABEL. Sie unterstützen Unternehmen in allen IT- und datenschutzrechtlichen Fragestellungen.



Sicherheitsoptionen in TeamViewer konfigurieren

Alle Screenshots: Thomas Joos

Videokonferenzsysteme

Datenschutz bei TeamViewer umsetzen

Mit der deutschen Software TeamViewer lassen sich Fernwartungsaufgaben erledigen. Was viele nicht wissen: Die Software bietet auch einige Funktionen für das Homeoffice, etwa Webkonferenzen.

TeamViewer hat nahezu alles, was Anwender im Homeoffice benötigen. Die Benutzer können schnell und einfach von zu Hause oder unterwegs auf ihren geschäftlichen bzw. dienstlichen PC zugreifen. Zusätzlich bietet TeamViewer Möglichkeiten zur Gruppenarbeit und für Webkonferenzen. Außerdem lassen sich Dateien übertragen. Da bei all diesen Tätigkeiten der Datenschutz eine wichtige Rolle spielt, ist es durchaus sinnvoll, zu einer deutschen Software zu greifen.

Sicherheitsrisiken beim Einsatz von TeamViewer

Mit TeamViewer arbeiten sehr viele Unternehmen und Anwender. Das ist auch Hackern nicht entgangen. Da Anwender mit TeamViewer nahezu uneingeschränkt auf ihren Computer im Unternehmen zugreifen können, ist der heimische Rechner ein Einfallstor für Hacker und andere Angreifer. Übernimmt ein Angreifer den heimischen PC, kann er auch auf den Unternehmens-PC zugreifen. Das gilt v.a., weil sich Anmeldedaten für TeamViewer und Windows in der Software speichern lassen. Aus diesem Grund ist es wichtig, Anwender für die Gefahren zu sensibilisieren.

Im Internet kursiert eine Malware mit der Bezeichnung TeamSpy. TeamSpy versucht, über TeamViewer Angriffe auf Unternehmen zu starten. Abhilfe schafft, immer nur TeamViewer-Versionen von der offiziellen Anbieterseite zu nutzen oder die Software, die die IT-Abteilung im Unternehmen zur Verfügung stellt. Die Verbindung von Anwendern über TeamViewer erfolgt über Server des Anbieters. Auch sie sind generell angreifbar. Um möglichst sicher zu arbeiten, sollten Anwender vier Punkte beachten, die im Grunde generell gelten:

PRAXIS-TIPP

1. Keine unbekannten oder verdächtigen Anhänge aus E-Mails oder von Webseiten öffnen.
2. Überprüfen, ob Mails mit Anhängen von einem vertrauten Absender stammen. Das lässt sich recht einfach über die E-Mail-Domäne prüfen.
3. Keine Anmeldungen auf Webseiten für Remotedesktop-Dienste durchführen, wenn kein IT-Spezialist den Vorgang zuvor geprüft hat.
4. Keine Remote-Apps von unbekannten Quellen herunterladen.

Generell problematisch ist die Tatsache, dass TeamViewer in seinen Benutzerbedingungen nicht ausschließt, Google-Tracking-Tools einzusetzen. Grundsätzlich könnten also Daten in die USA übertragen werden. Auf Anfrage bekommen Unternehmen von TeamViewer einen Vertrag zur Auftragsverarbeitung.

Sicherheitsoptionen in TeamViewer überprüfen

Neben den genannten grundsätzlich geltenden vier Punkten können die Nutzer weitere Sicherheitsvorkehrungen treffen. Über „Extras“ ⇨ „Optionen“ steht ihnen in TeamViewer der Bereich „Sicherheit“ zur Verfügung.

- Hier sollten Anwender sicherstellen, dass das Kennwort für den persönlichen Zugriff so sicher wie möglich ist.
- Die Option „Einfachen Zugriff gewähren“ muss deaktiviert sein. Denn damit lassen sich Computer, die mit dem gleichen TeamViewer-Konto angemeldet sind, ohne Kennwortabfrage nutzen.
- Bei „Zufälliges Kennwort für spontanen Zugriff“ stellen die Anwender die Option „Sehr sicher (10 Zeichen)“ ein.
- Im Bereich „Regeln für Verbindungen zu diesem Computer“ sollte bei „Windowsanmeldung“ die Option „Nicht zugelassen“ aktiv sein.

Datenschutzeinstellungen

Mit TeamViewer lassen sich auch Webmeetings abhalten. Hier müssen Anwender darauf achten, dass die automatische Aufzeichnung solcher Meetings deaktiviert ist. Diese Einstellungen sind unter „Fernsteuerung“ ⇨ „Fernsteuerungsvoreinstellungen“ über „Sitzungsaufzeichnung automatisch starten“ und unter „Meeting“ ⇨ „Meeting Voreinstellungen“ bei „Meetings automatisch aufzeichnen“ zu finden.

Wichtig sind zudem die Einstellungen bei „Erweitert“. Hier lässt sich festlegen, wie oft TeamViewer nach Updates sucht. Um Sicherheitslücken schnell zu schließen, muss das Intervall möglichst kurz sein. Weitere wichtige Optionen finden sich im Bereich „Zugriffskontrolle“. Hier sollte zunächst restriktiv vorgegangen werden („Verbiete eingehende Fernsteuerungssitzungen“), außer Anwender benötigen Zugriff von zu Hause auf ihren Unternehmens-PC. „Details“ zeigt an, welche Rechte Anwender haben, wenn sie die aktuelle Auswahl bei „Zugriffskontrolle“ beibehalten.

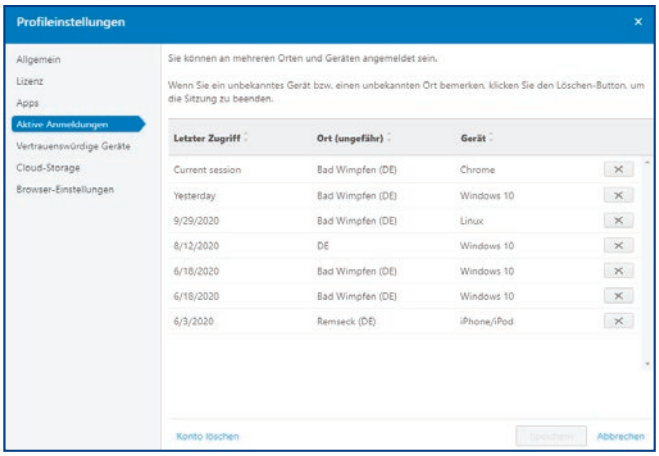
Viele Einstellungen in diesem Bereich sind selbsterklärend und sollten möglichst sicher konfiguriert werden. Dazu gehört z.B. die Option „Online-Status für diese TeamViewer ID verbergen“. Wichtig sind für das Nachverfolgen der Sicherheit auch die Optionen „Ereignisprotokoll aktivieren“, „Ausgehende Verbindungen protokollieren“ und „Eingehende Verbindungen protokollieren“ bei „Log-Dateien“.

Um die TeamViewer-Einstellungen zentral zu schützen, kann die IT bei „TeamViewer Einstellungen“ die Option „Der Zugriff auf die TeamViewer Optionen ist nur mit Administratorrechten möglich“ aktivieren.

Vertraute Geräte konfigurieren

Arbeiten Anwender mit einem TeamViewer-Konto, können sie sich an allen PCs anmelden, bei denen TeamViewer mit dem gleichen Konto gestartet wird. Damit die Anmeldung funktioniert, müssen die PCs als vertrautes Gerät „Trusted Device“ im TeamViewer-Konto hinterlegt sein.

Vor dem erstmaligen Zugriff versendet TeamViewer eine E-Mail an das entsprechende Konto. Über einen Link in dieser E-Mail kann der Anwender einen Computer als vertrautes Gerät hinzufügen. Hier sollten die Nutzer jedoch besonders skeptisch sein. Auf keinen Fall sollten sie einen Link anklicken, wenn sie nicht selbst den Computer hinzugefügt haben.

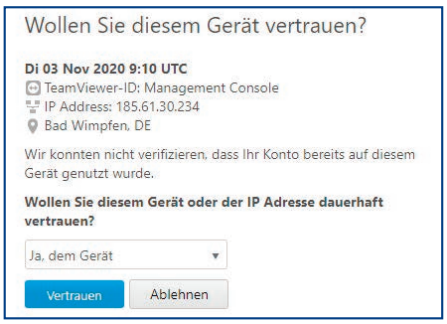


Anpassen der Sicherheitsoptionen in der Management Konsole

Außerdem sollten sie prüfen, ob die IP-Adresse stimmt. Die externe IP-Adresse lässt sich über verschiedene Dienste im Internet abfragen, etwa wieistmeineip.de. Bei der Auswahl von „Wollen Sie diesem Gerät oder der IP-Adresse dauerhaft vertrauen“ ist der sicherste Weg „Nein, nur einmalig“. Soll der PC häufiger genutzt werden, ist die Einstellung „Ja, dem Gerät“ sinnvoll.

TeamViewer Management Konsole richtig nutzen

TeamViewer stellt für seine Konten ein Webportal mit der Bezeichnung „TeamViewer Management Konsole“ zur Verfügung. Sie ist über https://login.teamviewer.com/ erreichbar. Ein Anmelden an der Konsole ist nur von vertrauten Computern aus möglich. Über die Konsole können Unternehmen, die eine TeamViewer-Lizenz haben, Richtlinien definieren. Das hat den Vorteil, dass die IT viele Sicherheits- und Datenschutzoptionen zentral für alle Clients vorgeben kann. Die Einstellungen sind bei „Anpassen & Ausrollen“ über die Registerkarte „Richtlinien“ zu finden.



Vertraute Geräte konfigurieren

Anwender können sich mit ihrem Konto ebenfalls an der Management Konsole anmelden und bei „Profil bearbeiten“ Sicherheitseinstellungen für ihr Konto konfigurieren. Besonders wichtig ist die Option „Zweifaktorauthentifizierung“ bei „Allgemein“. Außerdem lässt sich bei „Aktive Anmeldungen“ überprüfen, wann von den verschiedenen Geräten eine Anmeldung erfolgt ist. Bei „Meine Computer“ ist der Status der Computer zu sehen, die mit dem Konto angemeldet wurden. An dieser Stelle sollten nur aktuelle Computer zu sehen sein. Nicht mehr verwendete Computer sollten entfernt werden.

Sicherheit in Webmeetings

Anwender können im TeamViewer-Client bei „Meeting“ neue Meetings erstellen. Wichtig ist, ein sicheres Kennwort für den Zugang anzugeben. Startet der Ersteller ein Meeting, sieht er die anderen Benutzer. Er kann im Fenster die Rechte der einzelnen Teilnehmer einschränken. Über das Dropdown-Menü der Benutzer legt er fest, ob ein Benutzer Daten übertragen darf oder nicht. Administratoren können wiederum zentral über die Richtlinien in der Management Konsole steuern, ob z.B. das Aufzeichnen von Meetings erlaubt ist.

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

Bild: iStock.com/Jay_Zynism

Der Beitrag gibt einen Überblick über die datenschutzrechtlichen Anforderungen an Überwachungsmaßnahmen. Straf-, betriebsverfassungs- und telekommunikationsrechtliche Fragen klammert er dagegen aus.

Beschäftigtendatenschutz

Überwachung im Beschäftigtenverhältnis

Arbeitgeber haben regelmäßig ein nachvollziehbares Interesse daran, bestimmte Sachverhalte im Beschäftigtenverhältnis aufzuklären oder zu kontrollieren. Das gilt v.a. bei arbeitsvertraglichen Pflichtverletzungen oder Straftaten. Welche datenschutzrechtlichen Anforderungen an Überwachungsmaßnahmen gelten hier?

Eine Überwachung kann in vielen verschiedenen Formen erfolgen, etwa durch Technologien wie Videokameras oder durch den Einsatz von Menschen, etwa bei einer Taschenkontrolle. Um die personenbezogenen Daten der Beschäftigten zu schützen, sind dabei jedoch stets und von Anfang an die datenschutzrechtlichen Anforderungen, insbesondere die Vorschriften der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetz (BDSG), zu beachten.

Grundsätze von Art. 5 DSGVO als Leitfaden nutzen

Ausgangspunkt ist, dass weder die DSGVO noch das BDSG eine spezifische und abschließende Vorschrift zur Überwachung von Beschäftigten enthält. Zwar haben die europäischen und nationalen Gerichte sowie die Aufsichtsbehörden im Laufe der Jahre viele konkrete Anforderungen zu einzelnen Überwachungsmaßnahmen entwickelt. Jedoch fehlt es vielen Arbeitgebern und Datenschutzbeauftragten (DSB) nach wie vor an einer Art „Universal-Leitfaden", mit dem sich die datenschutzrechtliche Konformität jeder Überwachungsmaßnahme zumindest überblicksartig einordnen lässt.

Als Basis für einen solchen Leitfaden bieten sich die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 DSGVO an. Sie standardisieren den Schutz personenbezogener Daten der Beschäftigten und sind die allgemeinsten Anforderungen, die jede Verarbeitung personenbezogener Daten erfüllen muss.

Rechtmäßigkeit

Gemäß Art. 5 Abs. 1 Buchst. a DSGVO müssen Verantwortliche und Auftragsverarbeiter die personenbezogenen Daten auf rechtmäßige Weise verarbeiten. Die Verarbeitung ist nur dann rechtmäßig, wenn sie entweder eine der Rechtsgrundlagen aus Art. 6 DSGVO oder aus § 26 BDSG erfüllt.

Einwilligung

Grundsätzlich lässt sich eine Überwachungsmaßnahme auf eine Einwilligung des Beschäf-

tigten stützen. Dazu müssen die Voraussetzungen von Art. 6 Abs. 1 Buchst. a DSGVO, Art. 4 Nr. 11 DSGVO sowie ergänzend von § 26 Abs. 2 BDSG erfüllt sein.

Die zentrale Herausforderung liegt hierbei in der Freiwilligkeit der Einwilligung. Nach Erwägungsgrund 42 Satz 5 DSGVO lässt sich nur dann von einer freiwilligen Einwilligung ausgehen, wenn die betroffene Person eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind gemäß § 26 Abs. 2 Satz 1 BDSG für die Beurteilung der Freiwilligkeit der Einwilligung zu berücksichtigen

- die Abhängigkeit im Beschäftigungsverhältnis sowie
- die Umstände, unter denen der Mitarbeitende die Einwilligung erteilt hat.

Gemeinsam mit § 26 Abs. 2 Satz 2 BDSG betrachtet folgt daraus: Die Einwilligung ist nicht kategorisch ausgeschlossen. Sie ist allerdings stets im Kontext der konkreten Überwachungsmaßnahme zu prüfen.

Vertragserfüllung

Gemäß Art. 6 Abs. 1 Buchst. b DSGVO ist die Verarbeitung rechtmäßig, wenn sie erforderlich ist, um einen Vertrag zu erfüllen, dessen Vertragspartei die betroffene Person ist, oder um vorvertragliche Maßnahmen durchzuführen, die auf Anfrage der betroffenen Person erfolgen.

§ 26 Abs. 1 Satz 1 BDSG spezifiziert das aus der Perspektive des Beschäftigungsverhältnisses. Demnach dürfen Verantwortliche personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeiten, wenn dies erforderlich ist,

- um über die Begründung eines Beschäftigungsverhältnisses zu entscheiden oder
- um nach der Begründung das Beschäftigungsverhältnis durchzuführen oder zu beenden oder
- um Rechte und Pflichten der Interessenvertretung der Beschäftigten auszuüben oder zu erfüllen, die sich aus dem Gesetz, einem Tarifvertrag oder einer Kollektivvereinbarung ergeben.

Grundsätzlich sind bei der Prüfung der Erforderlichkeit die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.

Diese Abwägung hängt von den konkreten Umständen des Einzelfalls ab. Allerdings finden sich beispielsweise in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen" der Datenschutzkonferenz verschiedene konkrete Fragen bzw. Kriterien für Videoüberwachungsmaßnahmen (https://ogy.de/dsk-oh-videoueberwachung). Sie lassen sich entsprechend verallgemeinern:

- Besteht eine Gefährdungslage und auf welche Tatsachen, z.B. Vorkommnisse in der Vergangenheit, gründet sich diese?
- Warum ist die Überwachungsmaßnahme geeignet, den festgelegten Zweck zu erreichen?
- Warum ist die Überwachungsmaßnahme erforderlich und warum gibt es keine milderen Mittel, die für das Persönlichkeitsrecht der Betroffenen weniger einschneidend sind?
- Welche schutzwürdigen Interessen der Betroffenen haben Sie mit welchem Ergebnis in die Interessenabwägung einbezogen?
- Über welche technischen Möglichkeiten verfügt die Überwachungstechnologie und welche hiervon sind für die Überwachung nicht erforderlich und ggf. zu deaktivieren?

Rechtliche Verpflichtung

In seltenen Fällen kann auch eine rechtliche Verpflichtung des Arbeitgebers gemäß Art. 6 Abs. 1 Buchst. c DSGVO eine Rechtsgrundlage für Überwachungsmaßnahmen darstellen. Hierbei ist jedoch zu beachten, dass das zugrunde liegende Gesetz eine bestimmte Datenverarbeitung verpflichtend anordnen muss. Das ist nur in wenigen Konstellationen der Fall.

Beim sogenannten Terrorlisten-Screening verpflichten z.B. die entsprechenden EU-Verordnungen die Arbeitgeber nicht dazu, ihre Beschäftigten mit den gelisteten Personen zu ver- →

Freiwilligkeit bei einer Einwilligung

§ 26 Abs. 2 Satz 2 BDSG macht deutlich, dass Freiwilligkeit bei einer Einwilligung v.a. dann vorliegen kann, wenn der Beschäftigte einen rechtlichen oder wirtschaftlichen Vorteil erreicht oder Arbeitgeber und Beschäftigter gleich gelagerte Interessen verfolgen. Seine Überwachung wird einem Beschäftigten eher selten einen rechtlichen oder wirtschaftlichen Vorteil bringen – meist ist das Gegenteil der Fall. Etwas anderes gilt jedoch z.B., wenn der Beschäftigte betriebliche Kommunikationsmittel privat nutzen darf und er in diesem Zusammenhang in angemessene Kontrollen einwilligt. Auch können der Arbeitgeber und der Beschäftigte ausnahmsweise gleich gelagerte Interessen verfolgen. Das ist z.B. möglich, wenn es um die Videoüberwachung von besonders gefährdeten Objekten wie Tankstellen, Banken oder Geldtransportern geht.

gleichen, sondern sie verbieten nur bestimmte Interaktionen mit den gelisteten Personen. Der Umstand, dass der Arbeitgeber dafür notwendigerweise einen Abgleich durchführen muss, bleibt für Art. 6 Abs. 1 Buchst. c DSGVO unbeachtlich. Selbstverständlich kann das jedoch im Rahmen von § 26 Abs. 1 Satz 1 BDSG oder Art. 6 Abs. 1 Buchst. f DSGVO eine Rolle spielen.

Dagegen kommt eine Überwachung aufgrund einer rechtlichen Verpflichtung etwa im Rahmen von § 83 Wertpapierhandelsgesetz (WpHG) in Betracht. Wertpapierdienstleistungsunternehmen müssen nach § 83 Abs. 3 Satz 1 WpHG die Inhalte von Telefongesprächen und elektronischer Kommunikation aufzeichnen. Das gilt in bestimmten Fällen für Zwecke der Beweissicherung.

Berechtigte Interessen

Zulässig ist gemäß Art. 6 Abs. 1 Buchst. f DSGVO zudem die Verarbeitung zur Wahrung der berechtigten Interessen des Arbeitgebers oder eines Dritten. Voraussetzung: Die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen nicht. Hierbei handelt es sich um die zentrale Interessenabwägungsklausel der DSGVO. Sowohl die Struktur – berechtigte Interessen, Erforderlichkeit, Abwägung – als auch die Abwägungskriterien entsprechen im Beschäftigtenverhältnis weitgehend der Abwägung im Rahmen von § 26 Abs. 1 Satz 1 DSGVO (siehe oben „Vertragserfüllung").

Aufdeckung von Straftaten

Ein zentraler Erlaubnistatbestand mit Blick auf Überwachungsmaßnahmen ist § 26 Abs. 1 Satz 2 BDSG. Danach ist die Verarbeitung von personenbezogenen Daten zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat. Des Weiteren muss die Verarbeitung zur Aufdeckung erforderlich sein und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegen. Insbesondere dürfen Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sein.

Betriebsvereinbarung

Schließlich ist die Verarbeitung personenbezogener Daten gemäß § 26 Abs. 4 BDSG auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei ist jedoch Art. 88 Abs. 2 DSGVO zu beachten. Insbesondere kann auch eine Betriebsvereinbarung keine offensichtlich datenschutzrechtlich unzulässige Überwachung von Beschäftigten rechtfertigen.

Transparenz

Gemäß Art. 5 Abs. 1 Buchst. a DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die für die betroffene Person nachvollziehbar ist. Der Arbeitgeber muss daher grundsätzlich die Beschäftigten gemäß Art. 13 oder 14 DSGVO informieren. Das kann entweder im Rahmen der allgemeinen Datenschutzerklärung für Beschäftigte oder in Form von speziellen Datenschutzerklärungen für bestimmte Überwachungsmaßnahmen erfolgen. Insbesondere im Bereich der Videoüberwachung sollte der Arbeitgeber zudem die Vorgaben der Aufsichtsbehörden zur Ausschilderung der Videoüberwachung berücksichtigen.

Zweckbindung

Gemäß Art. 5 Abs. 1 Buchst. b DSGVO dürfen Verantwortliche personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erheben. Sie dürfen sie nicht in einer Weise weiterverarbeiten, die mit diesen Zwecken nicht zu vereinbaren sind. Für Überwachungsmaßnahmen bedeutet das zweierlei:

- Bereits erhobene Daten – also den Altdatenbestand – darf der Arbeitgeber nur zu Überwachungszwecken verwenden, sofern er dies schon zum Erhebungszeitpunkt als Verarbeitungszweck festgelegt hat oder wenn die ursprünglich festgelegten Zwecke und die Überwachungszwecke miteinander vereinbar sind. Letzteres ist an den Kriterien von Art. 6 Abs. 4 DSGVO zu messen.
- Bevor der Arbeitgeber neue Daten zu Überwachungszwecken erhebt, muss er diese Zwecke festlegen. Das erfolgt typischerweise intern, indem er die Verarbeitung ins Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 Buchst. b DSGVO aufnimmt. Extern erfolgt die Festlegung durch die Aufnahme in die Datenschutzerklärung nach Art. 13 Abs. 1 Buchst. c und 14 Abs. 1 Buchst. c DSGVO. An diese festgelegten Überwachungszwecke bleibt der Arbeitgeber zukünftig gebunden. Zweckänderungen sind nur un-

WICHTIG

Folgende Voraussetzungen muss der Arbeitgeber besonders sorgfältig prüfen, wenn er sich auf § 26 Abs. 1 Satz 2 BDSG stützt:

- *Die Straftat muss einen Bezug zum Beschäftigungsverhältnis aufweisen.*
- *Es müssen tatsächlich Anhaltspunkte existieren, die über vage Hinweise und bloße Mutmaßungen hinausgehen.*
- *Der Arbeitgeber muss diese tatsächlichen Anhaltspunkte genau dokumentieren.*
- *Die Überwachungsmaßnahme an sich muss verhältnismäßig sein.*
- *Der Arbeitgeber muss abwägen zwischen dem Aufklärungsinteresse einerseits und der Persönlichkeitsbeeinträchtigung des Arbeitnehmers andererseits. Kriterien dafür sind die Dringlichkeit des Tatverdachts, die Zahl der überwachten Arbeitnehmer und die Intensität der Maßnahmen.*

ter den Voraussetzungen von Art. 5 Abs. 1 Buchst. b und Art. 6 Abs. 4 DSGVO zulässig.

Datenminimierung

Gemäß Art. 5 Abs. 1 Buchst. c DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das Maß beschränkt sein, das für die Zwecke der Verarbeitung notwendig ist. Eine Anonymisierung von Daten ist für Überwachungszwecke regelmäßig nicht sinnvoll. Jedoch ist zu prüfen, ob die Überwachung nicht auf Grundlage von pseudonymisierten Daten im Sinne von Art. 4 Nr. 5 DSGVO erfolgen kann. Das kann insbesondere bei Data-Loss-Prevention-Tools der Fall sein.

Datenrichtigkeit

Gemäß Art. 5 Abs. 1 Buchst. d DSGVO müssen personenbezogene Daten sachlich richtig und auf dem neuesten Stand sein. Setzen Arbeitgeber Überwachungstechnologien ein, sollten sie ein besonderes Augenmerk darauf haben, „false positives", also Fehlalarme, zu vermeiden, zu überwachen und zu beheben.

Speicherbegrenzung

Gemäß Art. 5 Abs. 1 Buchst. e DSGVO müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Die DSGVO selbst definiert keine konkreten Speicherfristen. Der Arbeitgeber selbst muss sie festlegen und rechtfertigen. So müssen sich Unternehmen zunächst die Frage stellen, ob überhaupt eine Speicherung erforderlich ist, um die Überwachungszwecke zu erreichen, oder ob nicht ein Live-Monitoring ausreicht.

Sollte eine Speicherung erforderlich oder im konkreten Fall das mildere Mittel sein, hängt die jeweils zulässige Speicherdauer davon ab, wie rasch typischerweise das überwachte Fehlverhalten entdeckt wird. Setzt der Arbeitgeber z.B. Videoüberwachung ein, um tätliche Angriffe auf Beschäftigte aufzuklären, wird ein solches Verhalten normalerweise schnell bekannt sein. Dementsprechend ist auch nur eine relativ kurze Aufbewahrungsdauer gerechtfertigt.

Dagegen kann es z.B. bei komplexen Angriffen auf IT-Systeme durch Innentäter recht lange dauern, bis sie entdeckt werden. In solchen Fällen lässt sich zweckgebunden eine längere Speicherdauer rechtfertigen. Bei einem Rechtsstreit zwischen Arbeitgeber und Beschäftigtem können die Daten gemäß Art. 17 Abs. 3 Buchst. e DSGVO darüber hinaus für die Dauer des Prozesses aufbewahrt werden.

Datensicherheit

Gemäß Art. 5 Abs. 1 Buchst. e DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, dass ihre Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet ist.

Setzen Verantwortliche auf Überwachungsmaßnahmen, müssen sie die Vertraulichkeit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen sicherstellen. Das gilt in besonderem Maße, wenn sie ein vermutliches Fehlverhalten entdecken und untersuchen. Denn dieses Verdachtsstadium kann für den verdächtigten Beschäftigten besonders belastend sein. Es ist daher darauf zu achten, durch ein geeignetes Berechtigungskonzept nur einer begrenzten Anzahl von Personen Zugriff auf die Daten zu geben („Need-to-know"-Prinzip).

Rechenschaft

Gemäß Art. 5 Abs. 2 DSGVO ist der Arbeitgeber für die Einhaltung der beschriebenen Grundsätze verantwortlich und muss diese Einhaltung nachweisen können. Zwei Themen müssen Verantwortliche hierbei immer beachten:

- Zum einen muss der Arbeitgeber die Verarbeitungstätigkeiten im Zusammenhang mit der Überwachung in das Verzeichnis der Verarbeitungstätigkeiten aufnehmen.
- Zum anderen muss er vor Einführung der Überwachungsmaßnahme meist eine Datenschutz-Folgenabschätzung durchführen.

Schritt für Schritt vorgehen

Die datenschutzkonforme Überwachung von Beschäftigten ist nicht trivial. Allerdings stehen bewährte Mechanismen zur Verfügung, um einerseits die Effektivität der Überwachung zu gewährleisten und andererseits die Interessen der Beschäftigten zu berücksichtigen.

Constantin Herfurth arbeitet als Associate bei der Rechtsanwaltskanzlei Eversheds Sutherland. Seine Beratungstätigkeit umfasst das Datenschutz- und IT-Recht.

PRAXIS-TIPP

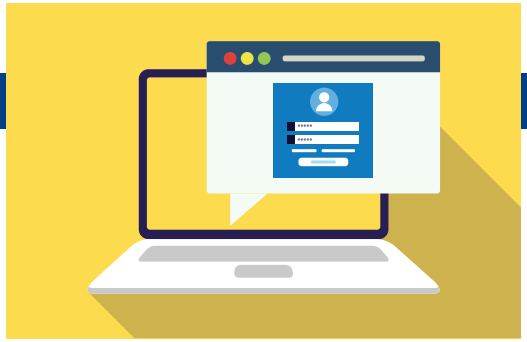
Die Pseudonymisierung verschleiert gezielt die Identität des einzelnen Beschäftigten mithilfe eines Pseudonyms. Im Normalfall bleibt der Beschäftigte somit gegenüber dem Arbeitgeber unerkannt. Ausschließlich im Fall eines bestimmten Fehlverhaltens wird die Identität des Beschäftigten nach einem festgelegten Verfahren aufgedeckt. Wichtig ist, die Verwaltung der Pseudonyme gesondert aufzubewahren und durch technische und organisatorische Maßnahmen zu sichern.

False positives (Fehlalarme) vermeiden

Es ist offensichtlich, dass Fehlalarme sowohl für den Arbeitgeber als auch für Beschäftigte prinzipiell unerwünscht sind. Für letztere können Fehlalarme jedoch nachteilige Folgen bedeuten. Aus diesem Grund sollten Arbeitgeber – insbesondere in der Anfangsphase – ihre Überwachungstechnologien selbst überwachen und die Fehlerrate kontrollieren, dokumentieren sowie bei Bedarf die zugrunde liegende Logik anpassen.

Datenschutzaufsicht Berlin

Abbruch einer Kundenregistrierung



Um eine Online-Bestellung bearbeiten zu können, ist eine Reihe von Daten des Kunden nötig. Häufig kommen dabei mehrstufige Registrierungsprozesse zum Einsatz. In einem Fall, den die Datenschutzaufsicht Berlin zu beurteilen hatte, wurde der Nutzer im ersten Schritt nach seiner E-Mail-Adresse und seinem Passwort gefragt, in drei weiteren Schritten dann nach zusätzlichen Daten. Jeder Schritt wurde mit einem Button „Speichern und weiter" beendet. Der Nutzer erhielt den Hinweis, dass die eingegebenen Daten gespeichert werden, damit er die Registrierung auch noch zu einem späteren Zeitpunkt abschließen kann.

E-Mail trotz Abbruch

Der Beschwerdeführer hatte die Registrierung abgebrochen. Später erhielt er trotzdem eine E-Mail des Unternehmens. Zur Frage, ob dies datenschutzrechtlich korrekt war, hält die Datenschutzaufsicht Berlin zunächst fest:

- Bricht jemand einen Registrierungsprozess ab, ist die fortgesetzte Speicherung der eingegebenen personenbezogenen Daten nicht ohne Weiteres zulässig.
- Zwar besteht ein berechtigtes Interesse von Plattformen, eine spätere Wiederaufnahme des Registrierungsprozesses zu ermöglichen. Es ist aber nicht erforderlich, die Daten aller Betroffenen, die den Registrierungsprozess abbrechen, zu speichern.
- Allein die Tatsache, dass ein Unternehmen über die Speicherung personenbezogener Daten informiert, führt nicht dazu, dass sie zulässig ist.

Empfehlungen der Aufsicht

Auf dieser Basis empfiehlt die Datenschutzaufsicht Berlin:

- Der Registrierungsprozess sollte einen Button wie „Abbrechen und Daten löschen" vorsehen.
- Ebenso sollte es einen ausdrücklichen Button wie „Daten speichern, um Registrierung später fortzusetzen" geben.
- Setzt jemand die Registrierung nicht fort, ohne einen dieser Buttons anzuklicken, müssen Websitebetreiber festlegen, ab welcher Zeit der Untätigkeit ein Abbruch anzunehmen ist.
- Hierbei kommt es auch darauf an, wie lange es dauert, das jeweilige Formular auszufüllen. Hinzuzurechnen ist eine angemessene Zeitspanne, um Störungen abzudecken.
- Eine datenschutzfreundliche Alternative wäre eine Server-Speicherung am Ende des Registrierungsprozesses.

Quelle: Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht für 2019, Nr. 9.10. Der Bericht ist abrufbar unter https://ogy.de/tb-berlin-2019

Bild: iStock.com/Alpaben Rathod

Streit im Verein

Herausgabe von Mitgliederlisten?

Der Sportverein Hannover 96 hat über 23.000 Mitglieder. Drei Vereinsmitglieder forderten vom Vorstand eine komplette Liste sämtlicher Mitglieder. Sie wollten alle Mitglieder kontaktieren, um Unterstützer für eine außerordentliche Mitgliederversammlung zu gewinnen. Als sich der Vorstand weigerte, beantragten sie beim Amtsgericht Hannover eine einstweilige Verfügung. Das Amtsgericht gab ihnen recht. Um die Festsetzung eines Zwangsgeldes durch das Amtsgericht zu vermeiden, gab der Vorstand die Mitgliederliste heraus. Nicht in ihr enthalten waren die Daten der Mitglieder, die gegenüber dem Verein einer Herausgabe ihrer Daten ausdrücklich widersprochen hatten.

Im Zuge des Gerichtsverfahrens hatte der Verein Unterstützung bei der Datenschutzaufsicht Niedersachsen gesucht. Sie vertrat folgende Auffassung:

- Die drei Mitglieder haben ein berechtigtes Interesse an der Herausgabe der Mitgliederdaten. Denn nur so können sie versuchen, „Mitstreiter" zu finden.
- Allerdings sind auch die Interessen der anderen Mitglieder zu berücksichtigen.
- Ein Ausgleich zwischen den Interessen beider Seiten ließe sich dadurch erreichen, dass ein Treuhänder die Daten erhält. Er würde die Daten speichern und könnte alle Mitglieder im Auftrag der Dreiergruppe anschreiben.

Verein muss Daten herausgeben

Das Gericht ließ sich von dieser Stellungnahme nicht beeindrucken. Es verurteilte den Verein dennoch zur Herausgabe der Mitgliederliste an die drei Mitglieder. Die „siegreichen Drei" waren jedoch von sich aus bereit, einen Rechtsanwalt als Daten-Treuhänder einzuschalten. Die Daten wurden ausschließlich ihm übergeben.

Zur Haltung der Datenschutzaufsicht siehe https://ogy.de/tb-niedersachsen-2019. Die Presseerklärung der „siegreichen Drei" findet sich unter https://ogy.de/pm-datentreuhaender. Der Rechtsstreit wäre wohl vermeidbar gewesen, hätten alle Beteiligten die längst vorhandene Rechtsprechung des Bundesgerichtshofs zum Thema stärker beachtet (siehe Ehmann, Datenschutz PRAXIS 01/2018, Seite 5).

Dr. Eugen Ehmann ist als Regierungspräsident von Unterfranken derzeit v.a. mit Corona beschäftigt. Der Datenschutz dient zur Entspannung in der Freizeit.

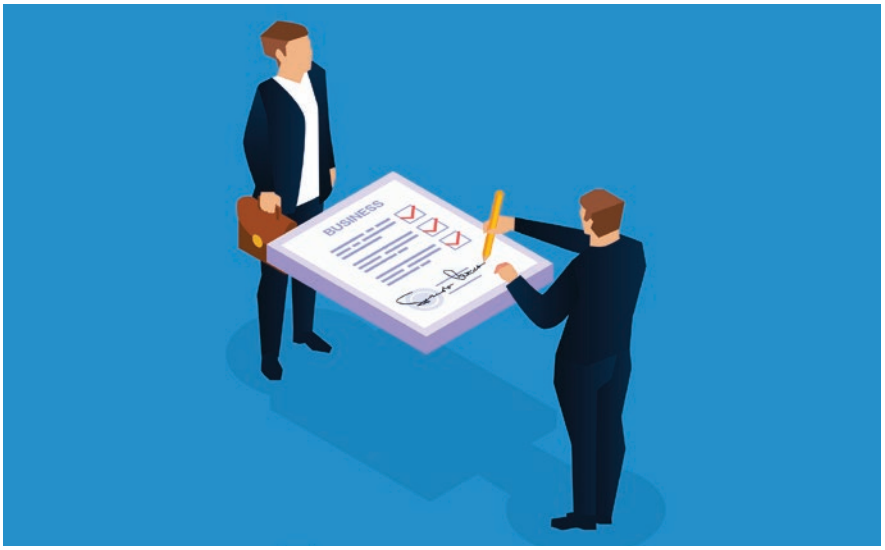


Bild: iStock.com/sesame

Wie können eigene Vorkehrungen Lücken im Datenschutzniveau bei der Datenübermittlung in Drittstaaten schließen? Wir nehmen die vertraglichen Maßnahmen unter die Lupe.

Vorschläge des EDSA

Ergänzende vertragliche Maßnahmen: Es wird konkret

Ergänzende Maßnahmen können vertraglicher, technischer oder organisatorischer Natur sein. Mehrere Instrumente zu kombinieren, ist oft sinnvoll. Wir konzentrieren uns auf die vertraglichen Maßnahmen.

Anhang 2 der Handreichung des Europäischen Datenschutzausschuss (EDSA) für ergänzende Maßnahmen bei der Datenübermittlung in Drittstaaten ist äußerst umfangreich. Er will konkrete Vorschläge dafür bieten, wie eigene Vorkehrungen Schwachstellen des Datenschutzniveaus etwa in den USA ausgleichen können.

Der Beitrag erläutert aus Anlage 2 den Teil der vertraglichen Maßnahmen. Er baut auf der Darstellung von Ehmann in der Ausgabe 01/2021 Seite 1 auf. Wichtige Stellen der Handreichung sind mit ihrer Randnummer (Rn) genannt. Sie ist online abrufbar unter https://ogy.de/supplementary-measures.

Bedeutung ergänzender Maßnahmen

Ergänzende Maßnahmen des Verantwortlichen sollen dafür sorgen, dass die Datenübermittlung in einen Drittstaat wie die USA rechtlich zulässig wird, obwohl dort nach EU-Maßstäben kein ausreichendes Datenschutzniveau herrscht. Ein Verantwortlicher ergreift solche Maßnahmen also in erster Linie im eigenen Interesse.

Gelingen sie ihm nicht in einem ausreichenden Umfang, darf er keine personenbezogenen Daten in den Drittstaat übermitteln (Rn 70). Tut er dies trotzdem, müsste die zuständige Datenschutzaufsichtsbehörde einschreiten und die Datenübermittlung untersagen.

Weit mehr als nettes Beiwerk

Vor diesem Hintergrund kann auch ein beträchtlicher Aufwand gerechtfertigt sein. Das gilt insbesondere dann, wenn ein Geschäftsmodell mit der Datenübermittlung in den Drittstaat steht und fällt. Die ergänzenden Maßnahmen entscheiden dann darüber, ob der Verantwortliche das Geschäftsmodell fortführen kann oder nicht. So gesehen kann der Begriff „ergänzende“ Maßnahmen in die Irre führen. Sie sind kein nettes Beiwerk, sondern Kernstück jeder Strategie für Datenübermittlungen in Drittstaaten wie beispielsweise die USA.

Ergänzung zu verschiedenen Rechtsgrundlagen möglich

Ergänzende vertragliche Maßnahmen können unabhängig davon sinnvoll sein, worin die Rechtsgrundlage für eine Übermittlung in ein Drittland besteht. Dies hebt die Handreichung hervor (Rn 92).

Besonders naheliegend sind ergänzende vertragliche Maßnahmen, wenn die Datenübermittlung auf der Grundlage der EU-Standardvertragsklauseln erfolgt. Beachten Sie dabei, dass diese Standardvertragsklauseln derzeit überarbeitet werden. Denkbar wäre jedoch auch, dass vertragliche Vereinbarungen verbindliche interne Unternehmensregelungen ergänzen. Solche Kombinationen dürften in der Praxis aber deutlich seltener gefragt sein.

Schwachstelle aller vertraglichen Maßnahmen

Allen vertraglichen Maßnahmen ist eine Schwachstelle gemeinsam: Sie wirken – wie jede vertragliche Regelung – immer nur zwischen den Parteien eines Vertrags. In der Regel sind das zwei Unternehmen, zwischen denen Daten übermittelt werden. Das eine im Europäischen Wirtschaftsraum (EWR), das andere in einem Drittstaat, etwa in den USA. →

In keiner Weise an solche Verträge gebunden sind die Behörden des Drittstaats. Weder Finanzbehörden noch Sicherheitsbehörden noch Geheimdienste lassen sich durch vertragliche Regelungen zwischen zwei Unternehmen davon abhalten, auf Daten zuzugreifen (Rn 58).

Das ist nichts Besonderes. Auch in Deutschland könnten zwei Unternehmen niemals durch eine Vereinbarung untereinander eine Staatsanwaltschaft oder ein Finanzamt daran hindern, auf bestimmte Daten zuzugreifen.

Vertragliches Verbot von Weiterübermittlungen

Bei flüchtiger Betrachtung könnte deshalb der Eindruck entstehen, dass vertragliche Vereinbarungen zwischen den Unternehmen, die an einer Datenübermittlung beteiligt sind, von vornherein so gut wie nichts bewirken. Dies trifft jedoch nicht zu, wie folgendes Beispiel zeigt, das die Handreichung nicht erwähnt.

Ein Unternehmen übermittelt Daten aus Deutschland an ein Unternehmen in Kanada. Für Kanada besteht ein Angemessenheitsbeschluss. Insofern ist eine Datenübermittlung dorthin kein besonderes rechtliches Problem (siehe Art. 45 Abs. 1 Satz 2 Datenschutz-Grundverordnung – DSGVO): Sie bedarf keiner besonderen Genehmigung. In einer Vertragsklausel untersagt der Datenexporteur dem Datenempfänger ohne jede Ausnahme, die Daten in ein anderes Drittland weiter zu übermitteln (Untersagung des „onward transfer"). Damit stellt er sicher, dass es nicht zu einer Weiterübermittlung in ein Drittland mit unzureichendem Datenschutzniveau kommt. Eine solche Weiterübermittlung personenbezogener Daten wäre nämlich unzulässig (siehe Art. 44 Abs. 1 Satz 1 Halbsatz 2 DSGVO).

Vertragliche Verpflichtung, bestimmte technische Maßnahmen zu ergreifen

Vertragliche Vereinbarungen sind ein geeignetes Instrument, um den Vertragspartner zu verpflichten, bestimmte technische Maßnahmen zu ergreifen, etwa Daten zu verschlüsseln. Als Faustregel gilt: Jede technische Maßnahme, die der Datenempfänger in einem Drittstaat durchführen soll, muss Gegenstand einer vertraglichen Verpflichtung sein (Rn 97/98). Ansonsten würde es sich um eine einseitige Zusage handeln, die sich in der Regel auch wieder einseitig widerrufen lässt.

Vertragsstrafen

Für Verstöße gegen vertragliche Verpflichtungen können die Vertragspartner Vertragsstrafen vereinbaren. Diese Strafen sind in der Praxis ein sehr effektives Mittel, um die Einhaltung vertraglicher Verpflichtungen durchzusetzen. Im Zusammenhang mit der Verpflichtung zu technischen Maßnahmen erwähnt die Handreichung dieses Mittel nicht.

Verpflichtung, Transparenz über die Rechtslage herzustellen

Der Vertrag über eine Datenübermittlung in ein Drittland lässt sich um Anhänge ergänzen, die Klarheit darüber schaffen, welche Zugriffsrechte öffentliche Stellen im Zielland haben (Rn 99). Die Informationen für diese Anhänge sollte dabei der Datenimporteur liefern. Der Datenexporteur wird sie oft kaum beschaffen können.

Solche Anhänge könnten zeigen, dass der Datenexporteur seine Verpflichtung erfüllt hat, das Datenschutzniveau im Drittland einzuschätzen (Prinzip der Verantwortlichkeit, Art. 5 DSGVO). Sie sind ein Hilfsmittel für die Risikobewertung und dienen dem Datenexporteur, nicht den betroffenen Personen.

Erklärung des Datenimporteurs zu „Backdoors"

Der in der EDV allgemein übliche Fachbegriff „Backdoor" bezeichnet verborgene Zugriffsmöglichkeiten, über die z.B. staatliche Stellen an Daten gelangen können. Die Handreichung schlägt eine vertragliche Bestätigung des Datenimporteurs vor, dass er solche Hintertüren jedenfalls nicht bewusst geschaffen hat (Rn 103). Dabei erwähnt sie, dass das Recht mancher Länder es verbietet, die Existenz einer Backdoor zu offenbaren (Rn 104).

Für den Fall, dass der Datenimporteur seiner Informationspflicht nicht korrekt nachkommt, schlägt die Handreichung vor, Vertragsstrafen zu vereinbaren. Auch die Möglichkeit, den Vertrag fristlos zu kündigen, könnten die Vertragsparteien für diesen Fall vereinbaren (Rn 104). Beides kann allerdings einen bereits erfolgten Zugriff auf Daten nicht beseitigen.

Verpflichtung, Rechtsbehelfe zu ergreifen

Nach den Maßstäben des EU-Rechts und des Rechts der EU-Mitgliedstaaten ist es selbstverständlich, dass staatliches Handeln zumindest prinzipiell gerichtlich überprüfbar ist. Aus dieser Sicht liegt es nahe, den Datenimporteur zu verpflichten, bei Datenzugriffen von staatlichen Stellen im Drittland den Rechtsweg zu beschreiten (Rn 112).

Die Handreichung nennt aber sehr ehrlich die Grenze, an die ein solches Vorge-

Denkbare vertragliche Maßnahmen

Vertragliche Maßnahmen können unterschiedliche Zwecke verfolgen. Die Handreichung unterscheidet vier Zielrichtungen vertraglicher Maßnahmen:

1. **Verpflichtung des Datenimporteurs, bestimmte technische Schutzmaßnahmen zu ergreifen (Rn 97/98)**
2. **Verpflichtung des Datenimporteurs, Transparenz über die Rechtslage im Zielland herzustellen (Rn 99–111)**
3. **Verpflichtung des Datenimporteurs, Rechtsbehelfe gegenüber staatlichen Stellen zu ergreifen (Rn 112–115)**
4. **Unterstützung betroffener Personen durch den Datenimporteur bei der Wahrnehmung ihrer Rechte (Rn 116–121)**

Grundsätzliche Schwachstelle

Schweigeverpflichtungen

Mit dem Stichwort „Schweigeverpflichtung" spricht die Handreichung ein generelles Problem bei vertraglichen Vereinbarungen an. Viele Rechtsordnungen (etwa das Recht der USA) kennen Regelungen, wonach staatliche Stellen Unternehmen und einzelnen Privatleuten Schweigeverpflichtungen auferlegen können.
Über den Gegenstand dieser Schweigeverpflichtung dürfen sich die Betreffenden dann in keiner Weise nach außen äußern. Ansonsten haben sie rechtliche Konsequenzen zu befürchten, bis hin zu strafrechtlichen Folgen.

Gag Orders und National Security Letters

Die Handreichung geht hier nicht sehr in die Tiefe. Gerade beim Datenexport in die USA stellt sich dieses Problem jedoch in einem Ausmaß, das für den durchschnittlichen Europäer nur schwer vorstellbar ist. Schweigeverpflichtungen sind dort oft in National Security Letters enthalten (siehe dazu https://de.wikipedia.org/wiki/National_Security_Letter), von denen jedes Jahr Zehntausende ausgestellt werden. Ein Verstoß gegen eine darin enthaltene „Gag Order" (wörtlich: Knebelverfügung) kann im Extremfall sogar eine Haftstrafe nach sich ziehen. Risikolos ist es dagegen, wenn der Datenimporteur die entsprechende Rechtslage allgemein in einem Anhang zum Vertrag erklärt.

Bild: iStock.com/Mykyta Dolmatov

hen häufig stößt (Rn 113): Oft sind solche Zugriffe nach den rechtlichen Maßstäben des Drittlandes nicht zu beanstanden, lassen sich aber gleichwohl mit den Rechtsgrundsätzen der EU nicht vereinbaren. Die effektive Schutzwirkung von Verpflichtungen des Datenimporteurs, rechtliche Schritte zu ergreifen, ist dann gleich null.

Das Beispiel der USA

Das Recht der USA bietet dafür ein gutes Beispiel. Es ist keineswegs so, dass Einrichtungen wie die National Security Agency (NSA) Abhörmaßnahmen völlig nach eigenem Ermessen durchführen dürften. Für viele Vorgehensweisen ist vielmehr eine gerichtliche Zustimmung nötig.

Zuständig hierfür ist der United States Foreign Intelligence Surveillance Court (teils als FISC, teils als FISA-Court bezeichnet). Die Entscheidungen des Gerichts erfolgen dabei jedoch nach gesetzlichen Maßstäben, die aus EU-Sicht deutlich unzureichend sind (siehe dazu den Kasten bei Rn 45 unter Bezug auf die Entscheidung des Europäischen Gerichtshofs „Schrems II").

Unterstützung betroffener Personen, ihre Rechte wahrzunehmen

Die Rechte betroffener Personen sind v.a. dann gefährdet, wenn staatliche Stellen des Drittlands auf ihre Daten zugreifen. Die Handreichung schlägt vor, jedenfalls die freiwillige Herausgabe von Daten an staatliche Stellen an die Zustimmung der betroffenen Person und/oder des Datenexporteurs zu knüpfen (Rn 116). Oft verbieten es jedoch Rechtsvorschriften des Drittstaats, über Aufforderungen einer staatlichen Stelle zur freiwilligen Herausgabe auch nur zu sprechen. Dann ergeben solche Vereinbarungen keinen Sinn.

An solchen Rechtsvorschriften scheitern oft auch Vereinbarungen, nach denen der Datenimporteur den Datenexporteur darüber informieren muss, dass staatliche Stellen den Zugriff auf Daten fordern (Rn 118/119).

Hier flüchtet sich die Handreichung in die problematische Alternative, dass eine Information der betroffenen Personen jedenfalls dann erfolgen soll, wenn die Verpflichtung zur Geheimhaltung weggefallen ist. Das dürfte der betroffenen Person im Normalfall wenig helfen. Es wirkt für sie wohl eher frustrierend, dass etwas hinter ihrem Rücken abgelaufen ist, ohne dass sie davon wusste und etwas dagegen unternehmen konnte.

PRAXIS-TIPP

Für sich genommen können ergänzende vertragliche Regelungen kaum ein ausreichendes Schutzniveau bewirken. Auf der anderen Seite sollte man sehen, dass technische und organisatorische Maßnahmen rechtlich gesehen gewissermaßen „in der Luft hängen", wenn sie nicht durch vertragliche Regelungen verbindlich vorgeschrieben sind.
Bei der Festschreibung von Informationspflichten ist zu beachten, dass die bloße Information über eine Rechtsverletzung die Rechtsverletzung selbst nicht mehr aus der Welt schaffen kann. Insofern bringen nur solche Informationspflichten etwas, die Rechtsverletzungen noch verhindern können. Stets stoßen Informationspflichten an ihre Grenzen, wenn staatliche Vorschriften die Weitergabe der Information verbieten.
Berücksichtigen Sie diese Grenzen, können ergänzende vertragliche Regelungen im Ergebnis jedoch einen wesentlichen Beitrag dazu leisten, dass ein angemessenes Datenschutzniveau vorhanden ist.

Dr. Eugen Ehmann hat als Moderator alle der bisher fünf Deutsch-Amerikanischen Datenschutztage begleitet.

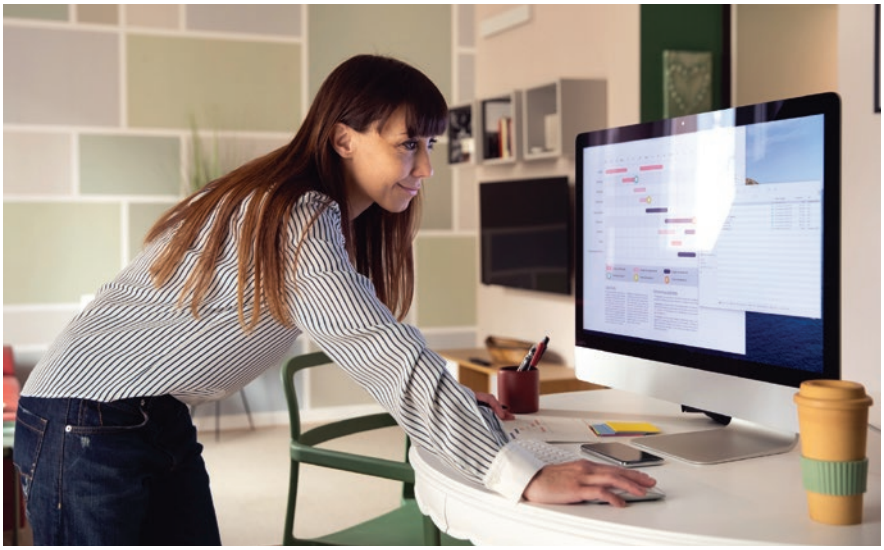


Bild: iStock.com/LeoPatrizi

Verantwortliche können Gruppenkalender im Einklang mit dem Datenschutz einführen. Das setzt voraus, dass der Arbeitgeber den DSB sowie den Betriebs- bzw. Personalrat einbindet und sich an einige datenschutzrechtliche Spielregeln hält.

Verpflichtende Öffnung ist ein Risiko

Der Gruppenkalender als Überwachungstool?

Elektronische Gruppenkalender sind Unternehmensalltag und erleichtern die Zusammenarbeit. Das gilt umso mehr in Zeiten von Corona, wo Flexibilität und Mobilität gefragt sind. Doch wie sind sie zulässig?

Ein Gruppenkalender oder die Freigabe des eigenen Kalenders für andere Kollegen erleichtern es, Informationen auszutauschen. Außerdem spart es Zeit, da sich die Mitarbeiter problemlos über Termine austauschen und koordinieren können. Das optimiert den Ablauf.

Aber: Überwachung möglich

Die Kehrseite ist, dass jeder, der Zugriff hat, prüfen kann, ob der andere Kollege viele oder eher wenige Termine hat und ob er vielleicht über die Dauer oder Anzahl seiner Termine schummelt. Damit lässt sich der einzelne Mitarbeitende über den Kalender überwachen.

Ist es zudem möglich, die Inhalte der Termine einzusehen, steigen diese Risiken: Dann lässt sich zusätzlich kontrollieren, welche Termine die Kollegin oder der Kollege tatsächlich wahrgenommen hat und ob die Angaben im Kalender mit den Aussagen beispielsweise gegenüber dem Vorgesetzen übereinstimmen.

Bestätigung durch Gericht

Das Verwaltungsgericht (VG) Sigmaringen hat diese Auffassung – die übrigens die Gerichte bereits seit längerer Zeit vertreten – jüngst bestätigt (siehe VG Sigmaringen, Beschluss vom 28. Juli 2020, PL 11 K 4795/18, https://ogy.de/urteil-kalender).

Der Gruppenkalender sei zur Überwachung von Mitarbeitern geeignet, da Vorgesetzte damit z.B. überprüfen können, ob der Beschäftigte stark oder wenig ausgelastet sei. Dieser Umstand könne im Rahmen einer Beurteilung des Mitarbeiters von Relevanz sein und damit letztlich in seine Beurteilung einfließen. Daraus abgeleitet entstehe für den einzelnen Mitarbeiter ein Überwachungsdruck.

Mitbestimmungspflichtig!

Daraus lässt sich eine Konsequenz ableiten, die die Rechtsprechung ebenfalls seit mehreren Jahren vertritt: Die Einrichtung eines Gruppenkalenders unterliegt der Mitbestimmung des Betriebs- oder Personalrats. Bereits die objektive Eignung zur Überwachung reicht für die Mitbestimmung aus. Das gilt unabhängig davon,

- ob der Arbeitgeber die Daten des Gruppenkalenders nur zu organisatorischen Zwecken nutzen will,
- ob er tatsächlich die Mitarbeiter überwacht oder
- ob der Überwachungsdruck aufgrund der minimalen Eingriffsintensität nur gering ist.

Verweigert der Verantwortliche die Mitbestimmung, können Betriebs- oder Personalrat die Nutzung bzw. Einführung des Gruppenkalenders blockieren.

Freigabe durch DSB reicht nicht

Interessant war an der Entscheidung des VG Sigmaringen zudem, dass der Datenschutzbeauftragte (DSB) des Verantwortlichen den Betrieb und Austausch von Daten über den Gruppenkalender als datenschutzrechtlich zulässig erachtet hatte. Das Gericht hat hier ausdrücklich darauf abgestellt, dass die Freigabe durch den DSB neben der Mitbestimmung des Betriebs- bzw. Personalrats steht und sie nicht ersetzen kann – ein Umstand, der zwar jedem Arbeitsrechtler geläufig ist, aber nicht jedem Geschäftsführer.

Im Ergebnis: Beide fragen!

Damit müssen Unternehmen bzw. Behörden zwei Dinge klären, bevor sie einen Gruppenkalender einführen:

- Mit dem Betriebs- bzw. Personalrat muss der Arbeitgeber u.a. abstimmen, welche Daten er wie von wem für welchen Zweck und für welche Dauer verarbeiten darf bzw. ob und welche Leistungs- und Verhaltenskontrollen erfolgen dürfen.
- Mit dem DSB ist abzuklären, ob und wie die geplante Verarbeitung von personenbezogenen Daten im Gruppenkalender datenschutzrechtlich zulässig ist.

Was gilt datenschutzrechtlich?

Setzt ein Unternehmen oder eine Behörde einen Gruppenkalender ein, verarbeitet es Daten von Mitarbeitenden zunächst intern. Als Rechtsgrundlage für den Umgang mit diesen Beschäftigtendaten kommt Art. 88 Datenschutz-Grundverordnung (DSGVO) in Verbindung mit § 26 Bundesdatenschutzgesetz (BDSG) in Betracht. Hier lässt sich argumentieren, dass ein Gruppenkalender erforderlich ist, um das Beschäftigungsverhältnis durchzuführen. Denn er ist ein Erfordernis, um den Betriebsablauf zu organisieren.

Im Rahmen der Verhältnismäßigkeitsprüfung muss der Verantwortliche abwägen, ob der Überwachungsdruck, der davon ausgeht, den Gruppenkalender für andere Mitarbeitende zu öffnen, bzw. ob die Möglichkeit der Kontrolle als so hoch einzustufen ist, dass er gegenüber den betrieblichen Erfordernissen bzw. Erleichterungen überwiegt. Dabei ist zu berücksichtigen, ob gleichwertige alternative Maßnahmen umsetzbar sind, wie z.B. tägliche Abstimmungen.

Wer darf zugreifen?

Wie hoch der Überwachungsdruck ist und ob der Gruppenkalender verhältnismäßig ist, hängt auch davon ab, wer auf den Kalender zugreifen darf und wie der Verantwortliche den Grundsatz der Integrität und Vertraulichkeit, den Art. 5 Abs. 1 Buchst. f DGSVO fordert, umsetzt.

Der Arbeitgeber sollte darauf achten, Zugriffsberechtigungen nur nach dem Need-to-know-Prinzip zu erteilen. Es empfiehlt sich, die gegenseitige Berechtigung zur Einsicht z.B. jeweils auf Kollegen solcher Bereiche zu beschränken, die zusammenarbeiten, oder sogar nur auf einzelne Kollegen oder Vorgesetzte.

Was ist mit dem Inhalt?

Wesentlich ist auch, welche Termine die Mitarbeitenden einstellen und ob alle deren Inhalt sehen. Während der Vertrieb vielleicht ein Interesse daran hat, zu wissen, welche Kunden der andere Kollege trifft, wird das bei einer Rechtsabteilung, die mit vertraulichen Dingen umgeht, nicht der Fall sein.

Der Arbeitgeber sollte immer die Möglichkeit bieten, die Termine ohne Inhalt (z.B. als Blocker oder maskiert) anzuzeigen. Das gilt erst recht, wenn die Mitarbeitenden auch private Termine eintragen. Der Arbeitgeber gibt idealerweise vor, diese Termine nur ohne Inhalt einzugeben oder – wenn dies systemseitig möglich ist – sie zu maskieren bzw. zu blockieren.

Zudem stellt sich gerade bei privaten Terminen die Frage, ob das Beschäftigungsverhältnis diese Verarbeitung noch abdeckt – hier wird wohl eher Art. 6 Abs. 1 Buchst. f DSGVO (berechtigtes Interesse) als Rechtsgrundlage heranzuziehen sein, nicht § 26 BDSG.

ACHTUNG!

Kritisch ist, wenn der Arbeitgeber die Mitarbeitenden anweist, den Gruppenkalender zu nutzen und Termine zwingend einzugeben. Das darf er nur, wenn er vorab den Betriebs- oder Personalrat eingebunden hat. Können die Mitarbeitenden zudem nicht freiwillig entscheiden, wer auf ihren Kalender zugreifen darf, sollten Sie als DSB eine gut dokumentierte und strukturierte datenschutzrechtliche Verhältnismäßigkeitsprüfung durchführen.

Silvia C. Bauer ist Rechtsanwältin bei der Luther Rechtsanwaltsgesellschaft mbH in Köln.

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.:
09100-4085

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.

Flurfunk auf Sendung

AU-Bescheinigung auf Abwegen

Bald heißt es schrittweise Abschied nehmen von der papierenen Arbeitsunfähigkeitsbescheinigung, auch AU-Bescheinigung genannt. Ursprünglich für den 1.1 geplant, aber verschoben, müssen Ärzte die AU-Bescheinigung nun ab dem 1.10.2021 digital an die Krankenkasse übermitteln. Ab Juli 2022 kann der Arbeitgeber zukünftig die Bescheinigung digital abrufen. Ob so manche Geschichte dann nicht mehr passiert?

Manche Beschäftigte schicken die Arbeitsunfähigkeitsbescheinigung brav per Post – und die Post wird wieder einmal verspätet zugestellt. Andere geben ihre „Krankmeldung" einem Kollegen mit, der in der Nachbarschaft wohnt. Dieser gibt sie dann im schlechtesten Fall einfach irgendjemandem beim Verantwortlichen.

Oft allzu große Sorglosigkeit

So kommt es dann dazu, dass am Empfang offen hingelegte „gelbe Zettel" für jedermann einsehbar sind. Oder sie jeder Mitarbeiter auf dem Schreibtisch des Teamleiters, zu dem alle Zutritt haben, zufällig entdecken kann. Dabei lassen sich über den Arztstempel Rückschlüsse auf die mögliche Art der Erkrankung ziehen.

Zu viel des Guten

Stellen Sie sich folgende Situation vor: Ein Kollege ist frisch verliebt und möchte imponieren. Voller Elan geht es im Fitnessstudio richtig zur Sache. Obwohl der Trainer sagt, er solle mit den Gewichten 80 Wiederholungen machen, macht er 120. Obwohl er 30 kg auflegen soll, nimmt er 40. Und so geht das den ganzen Abend.

Am nächsten Tag spürt er von der Schulter über den Ellenbogen bis in den kleinen Finger einen ziehenden Schmerz. Getreu dem Motto „Alter Indianer kennt keinen Schmerz" hält er das für eine Sehnenentzündung und glaubt, es ginge von allein weg. Nach drei Tagen ist er bei seinem Hausarzt. Der schickt ihn zum Neurologen. Die Sehne als Ursache fällt weg, das sieht wohl eher nach einer Nervenentzündung aus.

Verräterischer Arztstempel

Der Neurologe schreibt ihn auch sofort arbeitsunfähig. Er erhält eine AU-Bescheinigung, auf der als Arztstempel „Facharzt für Psychiatrie und Neurologie" zu sehen ist. Sie können sich sicher eine ungefähre Vorstellung davon machen, was ein normalerweise gut informierter Flurfunk aus dieser Information macht, wenn er sie in die Finger bekommt.

Seit 2005 ist Eberhard Häcker selbstständig mit Schwerpunkt Datenschutzberatung. Er ist Mitbegründer von Team Datenschutz, Fachautor und Dozent sowie Geschäftsführer der HäckerSoft GmbH.

IN DER NÄCHSTEN AUSGABE

Chatbots

Wer Dialogsysteme mit „sprachlichen Fähigkeiten" einsetzt, darf die datenschutzrechtlichen Pflichten nicht vergessen.

Datenschutzaudit Homeoffice

Auch wenn keine reale Begehung möglich ist: Virtuelle Prüfungen führen ebenfalls zu aufschlussreichen Ergebnissen.

Windows 10 & Telemetrie

Eine Arbeitsgruppe der Aufsichtsbehörden hat die Telemetriefunktion bewertet und erste Ergebnisse veröffentlicht.