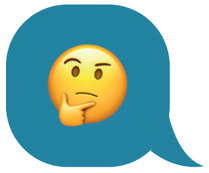
Ausgabe 01 | 2020

ExperSite
Das Magazin für Informationssicherheit und Datenschutz

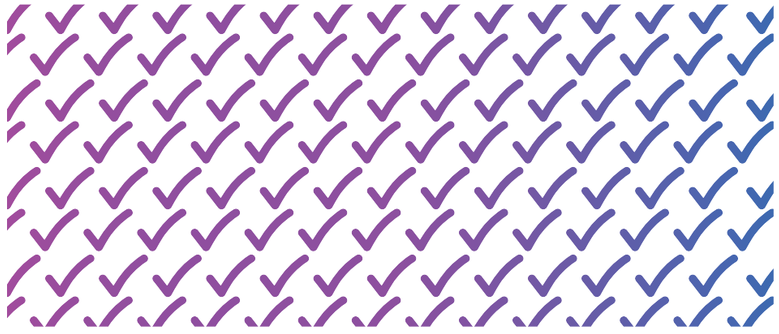
Zertifizierungen

Schön? Nützlich? Wertvoll?

Kam es zu einer Datenschutzverletzung, muss es anschließend schnell gehen. 10



Zwischen Autonomie und Abhängigkeit: Wieviel Kontrolle haben wir noch über unsere Daten? 26



DATATREE
YOUR COMPLIANCE PROVIDER

www.datatree.eu

Das Geschäft mit der Zertifizierung

Früher begann alles mit einem unverkennbaren Knacken, erst nach dem Bruch des Siegels erhielt man Zugriff auf wertvolle und zertifizierte Informationen. Seit Jahrtausenden vermittelt ein Siegel daher vor allen Dingen Sicherheit. Heute dient es unter anderem als Zeichen einer erfolgreichen Zertifizierung und garantiert hohe Qualitätsstandards. Ein Siegel gibt Kunden und Auftraggebern Orientierung und nach wie vor die oft verlangte Sicherheit. Insbesondere in Zeiten von Krisen und Pandemien, müssen durch die IT beeinträchtigte Bereiche verlässlich und sicher sein. Allerdings werden Siegel und Zertifizierungen inzwischen recht inflationär genutzt. Höchste Zeit, sich einen Überblick zu verschaffen.

Ein weiterer Schwerpunkt des Heftes beschäftigt sich mit unserem Umgang mit Daten – der ist nämlich gestört. Einerseits sind nach einer repräsentativen Umfrage des Max-Planck-Instituts die meisten Menschen benutzerdefinierter Werbung gegenüber offen, allerdings sind die wenigsten damit einverstanden, dass dafür persönliche Daten genutzt werden. So funktioniert das aber nicht. Wie es im Moment läuft, haben sehr gut norwegische Verbraucherschützer erkannt. Sie untersuchten beliebte Apps auf ihren Datenabfluss an Dritte, das Ergebnis finden Sie auf Seite 19. Nur so viel: Ein verantwortungsvoller Umgang mit personenbezogenen Daten sieht anders aus.

Auf gesetzlicher Ebene verlangen das IT-Sicherheitsgesetz oder auch die DSGVO die Zertifizierung als Qualitätsnachweis für beispielsweise Dienstleister. Wie schwer es trotz eines einheitlichen Rahmens ist, nach rein objektiven Gesichtspunkten zu bewerten, zeigt André Druch. Der Lehrer schildert die Herausforderung der Zertifizierung „Allgemeine Hochschulreife“ auf Seite 4.

„Siegel kann jeder vergeben.“

Ähnlich schwer gelingt Objektivität auch in anderen Bereichen der Zertifizierung und der damit einhergehenden Vergabe von Siegeln. Nicht immer stehen diese für Qualität. Es fehlen verbindliche Standards, dies nutzen einige schamlos aus. Es lohnt sich daher, genau hinzuschauen, was und nach welchen Kriterien zertifiziert wird. Nur weil die Tür oder Website eines Unternehmens mit einem vertrauenserweckenden Siegel geschmückt ist, bedeutet dies noch lange nicht, dass der für Sie relevante Unternehmensbereich auch Ihre Anforderungen erfüllt, ab Seite 23.

Ihre Nina Richard
(Redaktionsleitung)

Zwischen Verantwortung und Objektivität – aus dem Leben eines Lehrers

Was hat ein Lehrer mit Zertifizierungen zu tun? Mehr als man auf den ersten Blick glaubt. Das Zeugnis ist mit der Zertifizierung eng verwandt. In beiden Fällen wird eine erbrachte Leistung beglaubigt. In beiden Fällen entstehen von Fall zu Fall ganz unterschiedliche Herausforderungen auf dem Weg zur Beglaubigung.

Interview: Jörg Fecke

Herr Druch, mit dem ersten Zeugnis fängt es oft an, wir werden nach einem standardisierten Schema – den Schulnoten – beurteilt. Wieso ist das wichtig?

Zum einen handelt es sich bei dem Thema um ein weites konfliktbeladenes Feld. Diskussionen über das Für und Wider von Benotungen halten sich seit Jahrzehnten hartnäckig. Einiges ist aber auch unstrittig: Noten erfüllen eine ganze Reihe von Aufgaben. Zum einen dienen Schulnoten der Information. Schüler, aber vor allen Dingen auch Eltern, erhalten einen Einblick in den aktuellen schulischen Leistungsstand. Darüber hinaus wirken sich Schulnoten motivationsfördend aus und dienen nicht zuletzt als Zugangsmöglichkeiten, die nach Leistungen vergeben werden. Das Abitur wird einem z. B. nach wie vor nicht geschenkt.

Sie als Lehrer tragen eine große Verantwortung. Einerseits sollen Sie Kinder und Jugendliche auf ihr späteres Leben vorbereiten. Andererseits haben Sie mit ihren Einschätzungen auch einen maßgeblichen Einfluss auf das zukünftige Leben Ihrer Schüler. Wie gelingt es Ihnen, hier möglichst objektiv zu agieren?

Man muss sich als Lehrer immer bewusst sein, dass man immer versucht, so objektiv wie nur möglich Leistungen zu beurteilen. Eigene emotionale Gründe werden bewusst zurückgedrängt. Es wäre aber vermessen zu behaupten, dass man zu 100 % eine Beurteilung objektiv treffen kann. Darüber hinaus werden Schüler nicht mehr während des gesamten Unterrichts nach Noten beurteilt. In Übungsphasen steht der eigentliche Lernprozess im Vordergrund. Schüler sollen hier ausdrücklich Fehler machen und aus diesen dann ihre Schlüsse ziehen und so aus Fehlern lernen. Die primäre Funktion der Schule ist ja nicht die Erbringung von Leistungen, sondern das Lernen.

Die 100 % objektive Beurteilung ist Illusion

Sie unterrichten Deutsch und Sozialwissenschaften, die Korrektur einer Klausur stelle ich mir herausfordernder als z. B. im Fach Mathe vor. Wie gehen Sie hier vor, um eine richtige Benotung zu gewährleisten?

Das stimmt. Die Konsequenz: Es kostet mehr Zeit. In vielen Fällen handelt es sich um eine Abwägung. Dennoch, jede Klausur beruht auf einem Erwartungshorizont, aus diesem ergeben sich die idealen Antworten. Zwischen Idealantworten und den realen besteht mal mehr und mal weniger eine Diskrepanz. Man hat hier als Lehrer Interpretationsspielräume. Das führt dann dazu, dass gerade in Fächern wie Deutsch eine Korrektur bis zu 90 Minuten in Anspruch nimmt. Wenn Sie dann knapp 30 Schüler haben, entsteht zwangsläufig ein Zeitproblem.

Sie haben sowohl in der Erwachsenenbildung als auch an einem klassischen Gymnasium unterrichtet. Haben Sie da bei der Zeugnis- und Notenvergabe Unterschiede festgestellt?

Es gibt tatsächlich Unterschiede, die sich aus den verschiedenen Biografien ergeben. Man muss in der Erwachsenenbildung, besonders in der berufsbegleitenden Bildung, mehr Zugeständnisse machen. Faktoren wie Familie und Beruf wirken sich wesentlich stärker auf den Schulalltag aus, als das bei klassischen Schülern der Fall ist. Dies ist auch völlig normal. Das hat aber keinen Einfluss auf das Endergebnis. Für ein Abitur muss man einen gewissen Leistungsstand erreichen, unabhängig von der jeweiligen Schulform.

ANDRÉ DRUCH

André Druch arbeitet als Lehrer für Deutsch und Sozialwissenschaften seit acht Jahren an einem Gymnasium in Köln. Davor war er jahrelang an einem Aachener Weiterbildungskolleg tätig.

Sind denn Noten und Zeugnisse überhaupt notwendig?

Irgendeine Form der Beurteilung ist für Schüler und Eltern unablässig. Die Einordnung „was habe ich geschafft?“ vs. „was habe ich nicht geschafft“ stelle ich mir sonst schwierig vor. Gerade in meiner Klasse sind die Schüler ausgesprochen leistungsorientiert. Für die Schüler sind Noten daher als Kompass sehr wichtig. Nach meiner Einschätzung spielen Noten für die jetzigen Schüler eine größere Rolle als z. B. für mich als Schüler. Befriedigend wird heute in vielen Fällen als schlechte Note angesehen. Das war bei mir ehrlich gesagt nicht so ausgeprägt.

Haben Sie das Gefühl, dass ihre Beurteilungen nachvollzogen werden?

Ja, das gelingt sehr gut. Die Schüler haben durch die kommunizierten Erwartungshorizonte die Möglichkeit, sehr gut nachzuvollziehen, wir ihre Note entstanden ist. Jede Klausur wird kommentiert, sowohl die guten als auch die schlechten Aspekte. Auch einer der Gründe, wieso eine Korrektur inzwischen recht zeitintensiv ist.

Machen Sie sich mit der Notenvergabe in irgendeiner Weise auch angreifbar? Gut, einem Schüler mit mangelhaften Deutschkenntnissen werden Sie ja aller Voraussicht keine Zwei geben. Allerdings mehren sich Stimmen, dass Schüler auf die Zeit nach der Schule schlecht vorbereitet sind, trotz oftmals guter Noten. Wie ist Ihre Einschätzung?

Klar, das hört man schon regelmäßig. Mir persönlich ist das aber glücklicherweise noch nie passiert. Aber ich bin auch in einem relativ engen Kontakt mit den Schülern. Sprich, wir reden miteinander über Beurteilungen und Noten. Schüler haben auch Möglichkeiten, aktiv einzugreifen. Natürlich gebe ich eine Note nach bestem Wissen und Gewissen. Wenn Schüler allerdings anderer Meinung sind, dann können sie mit einer schriftlichen Begründung die aus ihrer Sicht ungerechte Benotung infrage stellen. Das kam schon mal vor. Wenn ich dann die Begründung nachvollziehen kann, dann berücksichtige ich das auch. Wer jetzt aber kommt und einfach nur sagt, dass er mit der Benotung nicht einverstanden ist, tja, das reicht ehrlich gesagt nicht ganz. Aufgrund dieser Transparenz macht man sich als Lehrer hinsichtlich der Noten auch nicht angreifbar.

Benotungen sind inzwischen sehr transparent

Gerade das Abitur hat in der öffentlichen Wahrnehmung gelitten. Oft wird ein Paradoxon beschrieben, dass es einerseits immer mehr Einser-Abiture gibt, aber andererseits die Schüler nicht die grundlegenden Voraussetzungen für ein Studium mitbringen. Wie passt das zusammen?

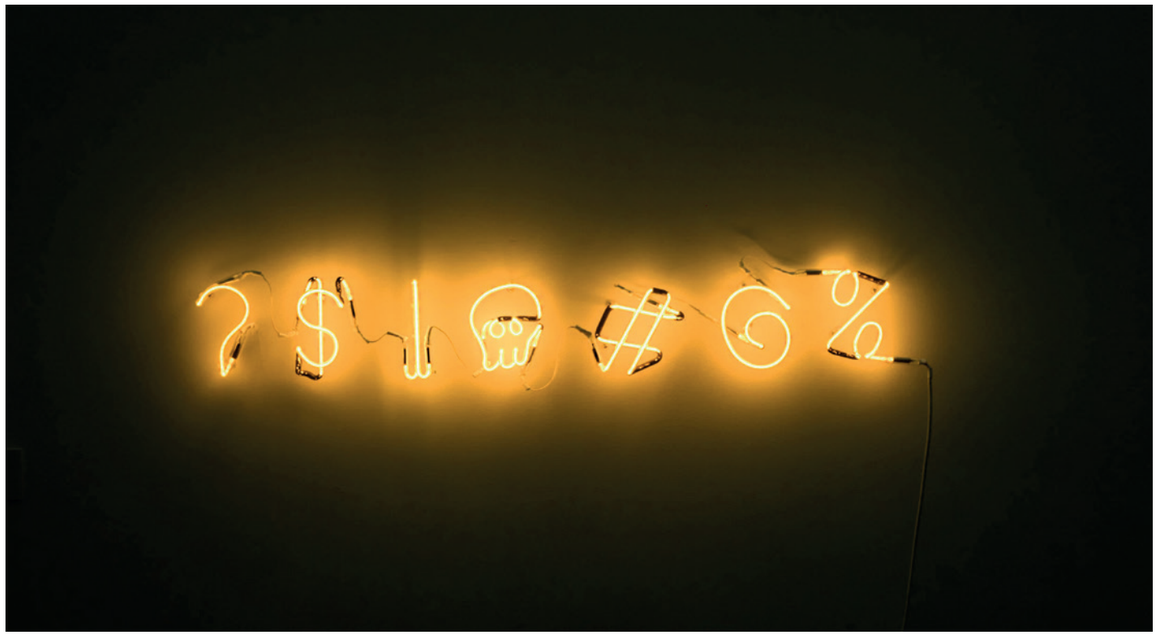
Tatsächlich glaube ich nicht, dass die Schüler von heute schlechtere Leistungen erbringen als früher, sie erbringen aber andere Leistungen. Der Unterrichtsinhalt ist heute komplexer. Die Aufnahmefähigkeit ist aber bei den Schülern über Generationen ähnlich. Natürlich werden dann andere Prioritäten gesetzt. Diktate gibt es bei uns so in der Form z. B. überhaupt nicht mehr. Auch das reine Auswendiglernen von Gedichten gibt es so nicht mehr.

Nach wie vor steht die Erlangung der allgemeinen Hochschulreife als finales Ziel fest. Viele glauben, dass damit ein Kanon an Kenntnissen gelernt wird. Also die bekannten Floskeln über Rechtschreibung und Grundrechenarten. Das stimmt aber nur zum Teil. Es geht nicht nur darum, möglichst fit für die Berufswelt gemacht zu werden – was heute durch Praktika und Schnuppertage in den Betrieben während der Schulzeit übrigens wesentlich besser funktioniert als noch vor einigen Jahren. Die allgemeine Hochschulreife ist vielmehr eine umfassende Bildung, eine kulturelle Bildung, eine soziale Bildung, eine Persönlichkeitsbildung. Das Abitur hat nicht nur einen ökonomischen, sondern einen gesamtgesellschaftlichen Auftrag, dem es gerecht werden muss. //

„DATENSCHUTZ-BEAUFTRAGTE SIND KEINE BEDENKEN-TRÄGER!“

Thomas Jäschke ist seit den 90er-Jahren als externer Datenschutzbeauftragter tätig. Nach wie vor arbeitet der promovierte Medizininformatiker als Datenschutzbeauftragter für namhafte Unternehmen, außerdem leitet er inzwischen ein erfolgreiches Datenschutz-Beratungsunternehmen. Seit dem ersten Job hat sich im Berufsbild des Datenschutzbeauftragten viel getan. Einige Konstanten bleiben bestehen. Höchste Zeit genauer zu fragen: Was macht einen guten Datenschutzbeauftragten aus?

Text: Nina Richard



„Neben Wissen und ständiger Fortbildung braucht es Mut und Lösungen."

Den Ausbildungsberuf oder das Studienfach Datenschutzbeauftragter gibt es nicht. Und selbst nach Besuch eines mehrtägigen Lehrgangs ist man noch lange nicht für die Praxis gewappnet. Jahrelange Erfahrung, Fortbildung auf eigene Faust und Interesse an verschiedensten Fachgebieten wie IT, Recht und diverse Softskills sind die Grundvoraussetzung, um einen guten Job zu machen. Und dann wären da noch die Geheimzutaten: Mut und Lösungsorientierung.

Als Datenschutzbeauftragter trägt man eine schwere Bürde. Die DSGVO wie auch das Leitbild der Datenschutzbeauftragten bringen vielfältige Aufgaben mit sich, die es zu erfüllen gilt. Zusätzlich wächst der Druck durch die Erwartungen, die Geschäftsführung und Kollegen/Mitarbeiter sowie Dienstleister und Kunden einem entgegenbringen. Wie man sich sieht und welche Verantwortung man übernimmt, kann man in gewissem Maße selbst bestimmen. Eine Sache steht allerdings fest: Bewegen kann man als Datenschutzbeauftragter viel, vorausgesetzt man kennt die eigenen Schwächen und Stärken.

Die Pflicht

Gesetzlich betrachtet ist der Datenschutzbeauftragte (DSB) gemäß Art. 39 DSGVO für die Beratung, Unterrichtung, Überwachung der gesetzlichen Vorgaben innerhalb des Unternehmens selbst sowie bei Dienstleistern und auch zusammen mit der Aufsichtsbehörde der DSGVO zuständig. Von der Mitarbeiterschulung über die Erstellung des VVT (Verzeichnis der Verfahrentätigkeiten) bis hin zur Datenschutzfolgenabschätzung. Die Aufgaben des Datenschutzbeauftragten sind vollumfänglich und in den wenigsten Fällen durch nur eine Person zu erfüllen.

„Eine Rezitation von Gesetzestexten ist nicht zielführend."

Die fachliche Ebene abzudecken, ist nur ein Bereich, den man als DSB beherrschen muss. Was bis heute allzu oft auf der Strecke bleibt, ist die Praxisorientierung. Aber woran liegt das? Ganz einfach: Es reicht eben nicht, das Gesetz zu kennen oder die Auslegung des Gesetzes auf juristischer Ebene durchzuführen, wenn die eigenen Kollegen nicht an juristischen Fachdiskussionen interessiert sind. Häufiger passiert es, dass Kollegen ein konkretes Problem haben und dann keine Rezitation der Gesetzeslage wünschen, sondern einen konkreten Umsetzungsvorschlag, z. B. in Bezug auf die Ausgestaltung einer Software oder die konkrete Prozessbeschreibung. Hier werden also tatsächlich Datenschutzbeauftragte benötigt, die fachübergreifend agieren und transferieren können.

Die drei Datenschutztypen

Achtung – stark vereinfachte Darstellung.

Der Branchenexperte

Der Branchenexperte kommt aus einem anderen Bereich, weit weg von Juristerei oder IT. Innerhalb seiner Fachabteilung hat er viel Erfahrung. Prozessgestaltung und Lösungen, die ihn und seine Kollegen jeden Tag weiter nach vorne bringen, sind Kern seiner Arbeit.

Der Informatiker

Je nach Schwerpunkt fühlt er sich zwischen Programmcodes oder den Komponenten der IT-Infrastruktur am wohlsten. Das Erarbeiten von Lösungen auf technischer Ebene ist sein Steckenpferd. Allerdings liegt ihm nicht immer die Auslegung der Gesetzestexte. Der Blick auf das große Ganze wird häufig vernachlässigt.

Der Jurist

Bei Gesetzestexten und deren Interpretation ist dieser Typ eine Koryphäe, ebenso wird die Rechtsberatung souverän abgedeckt. Häufig sind Detailarbeiten, wie die Gestaltung von Verträgen oder rechtssichere Argumentationslinien in Bezug auf eine Fallauslegung, genau seine Steckenpferde. Schwächen können hier häufig die praxisnahe Umsetzung und Durchführung von Lösungen sein, sprich – er kann Ihnen mitteilen, welche rechtlichen Aspekte Sie umsetzen müssen, allerdings nicht wie konkret eine technische Lösung programmiert wird und auszusehen hat.

„Das muss man wollen."

Alle drei Arten von Datenschutzexperten haben eine ausgezeichnete Kompetenz innerhalb ihrer Bereiche. Am Markt gefordert (Leitbild BVD), sind allerdings Personen, die alle oben aufgeführten Aspekte miteinander vereinen. Und das aus einem guten Grund: Das sind die Grundvoraussetzungen, um einen praxisnahen und funktionierenden Datenschutz zu leben. Weg vom immer noch weit verbreiteten „klassischen" Verhinderimage hin zum Möglichmacher. Ein Weg, den glücklicherweise bereits viele gehen. Leider allerdings noch nicht genug.

Und warum? Weil es ein Schritt raus aus der Komfortzone ist

Juristen, die sich in die hochkomplexe Thematik von Informationstechnologien einarbeiten müssen, Informatiker, die Gesetzestexte wälzen und deren Interpretation lernen müssen, oder Branchenexperten, die sich direkt noch zwei völlig neue Teilbereiche aneignen müssen. Das muss man wollen. Und bei all dem bleibt die frustrierende Erkenntnis: Niemand kann alles können – Datenschutzbeauftragte brauchen einander und den Austausch untereinander. //

72h

Souveräner Umgang mit Datenschutzverletzungen

Mit der Einführung des neuen Bußgeldmodells der Datenschutzbehörden sind Datenschutzverletzungen stärker in den Fokus der Öffentlichkeit geraten.

Deshalb gilt es, vorbereitet zu sein. Ab der Erkenntnis, dass potenziell eine Datenschutzverletzung vorliegen könnte, beginnt eine gesetzliche Frist von **72 Stunden**[1]. Auch wenn diese Frist zunächst lang erscheint, zeigt die Erfahrung, dass diese im Regelfall ausgeschöpft oder überschritten wird.

Damit dies nicht passiert, sollte man bereits vorab auf eine Datenschutzverletzung vorbereitet sein. Welche Grundprinzipien in diesem Kontext gelten, stellt der folgende Überblick dar.

Text: Ass.-Jur. Hanjo Tewes

Definition der Datenschutzverletzung

Die Datenschutzverletzung, auch die Verletzung des Schutzes personenbezogener Daten genannt, ist nach Art. 4 Nr. 12 DSGVO „eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden."

Auch wenn dieser Satz nur eine beschränkte Lesbarkeit hat, ist es dem Gesetzgeber gelungen, jede Form einer Datenschutzverletzung in einem Satz abzubilden.

Diese formelle Definition birgt im Berufsalltag allerdings eine Gefahr: Sie ist so formuliert, dass viele Personen bereits nach wenigen Worten inhaltlich abschalten.

Eine grobe Definition des Begriffes Datenschutzverletzung kann aber bereits mit wenigen einfachen Punkten gegeben werden. Lassen Sie sich hierfür auf ein kleines Experiment ein. Versuchen Sie direkt einzuordnen, ob es sich bei den folgenden Beispielen um Datenschutzverletzungen handelt.

BEISPIEL 1
Sie sind Patient. Zum Abschluss Ihrer Behandlung bekommen Sie einen Entlassbrief. Als Sie diesen öffnen, stellen Sie fest, dass der Brief mit der Diagnose und dem Behandlungsverlauf nicht Sie betrifft.

BEISPIEL 2
Sie kommen am Montagmorgen zur Arbeit und stellen fest, dass Ihr Passwort für den E-Mail-Account nicht mehr funktioniert. Als Sie auf den Systemadministrator zugehen, stellt dieser fest, dass in der Zeit, in der Sie im arbeitsfreien Wochenende waren, mehrfach auf Ihr persönliches Nutzerkonto zugegriffen wurde.

Die genannten Beispiele sind nicht komplex, zeigen jedoch, dass man innerhalb von wenigen Sekunden ein sicheres Gefühl dafür bekommt, ob es sich in den vorliegenden Fällen um eine Datenschutzverletzung handeln könnte. Dieses Gefühl ist in der Regel bei allen Mitarbeitenden vorhanden.

Hier gilt es, die Mitarbeitenden zu sensibilisieren und deren „Bauchgefühl" zu stärken. Dies kann durch das Besprechen von unternehmensinternen Beispielen geschehen. Gerade in den regelmäßig stattfindenden Schulungen kann anhand einer offenen Diskussion ein relativ großer Effekt erzielt werden, da so die abstrakte Definition des Gesetzes mit dem Alltag der Mitarbeitenden verknüpft und auf einer pragmatischen Ebene besprochen wird.

Außerdem muss ein kompetenter Ansprechpartner zur Verfügung stehen, der bei dem Problem einer potenziellen Datenschutzverletzung hilft. Dies sollte in der Regel der Datenschutzkoordinator oder Datenschutzbeauftragte sein.

Sofern die Mitarbeitenden Datenschutzverletzungen festgestellt haben, kann es vorkommen, dass sie sich überfordert fühlen oder aufgrund von eigenem Fehlverhalten das Problem schnell vergessen oder verschweigen möchten. Dies ist auch absolut nachvollziehbar.

Eine Datenschutzverletzung darf nicht zum Problem des Mitarbeitenden werden. Wenn Mitarbeitende sich melden, müssen sie das Gefühl haben, dass man hilft und Klarheit verschafft.

Potenzielle Datenschutzverletzung erkannt

Bei einer Datenschutzverletzung besteht grundsätzlich immer eine Meldepflicht gegenüber der Aufsichtsbehörde. Ab dem Zeitpunkt des Bekanntwerdens der Datenschutzverletzung muss die Datenschutzverletzung unverzüglich, spätestens aber innerhalb von 72 Stunden, gemeldet werden. 72 Stunden klingen zunächst ausreichend, gerade in größeren Unternehmen stellt sich jedoch die Herausforderung, dass bei potenziellen Datenschutzverletzungen direkt der Datenschutzkoordinator oder Datenschutzbeauftragte eingebunden werden muss.

Hier gilt es zu berücksichtigen, dass die Betriebsorganisation der verantwortlichen Stelle im Sinne des Datenschutzes zugerechnet wird. Dies bedeutet, dass sofern eine potenzielle Verletzung einem oder einer Mitarbeiter/-in bekannt wird, die Frist zu laufen beginnt.

Damit eine potenzielle Verletzung nicht wegen unklarer Melde-/Zuständigkeitsstrukturen verlorengeht, sollte eine direkte Ansprechperson benannt sein, welche die oben genannten Voraussetzungen erfüllt. Diese Person sollte in der Lage sein, die datenschutzrechtliche Einschätzung vornehmen und im Zweifelsfall unverzüglich die weiteren Schritte (Einbindung der GF; Meldung an das LDI etc.) initiieren zu können.

Bewertung des Vorfalls

Gerade die richtige Einschätzung des Vorfalls ist von großer Bedeutung. Die DSGVO geht zwar von einer grundsätzlichen Meldepflicht gegenüber den Aufsichtsbehörden aus, eine Meldung ist jedoch nicht vorzunehmen, wenn die Datenschutzverletzung nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt (Art. 33 Abs. 1 S. 2 DSGVO).

Für die Beurteilung des Risikos sind unter anderem die Schwere und die Eintrittswahrscheinlichkeit zu beachten.[2] In dieser Abwägung sind z. B. die Menge und die Art der betroffenen Daten, mögliche Ziele und Fähigkeiten Dritter, die die Daten erhalten, sowie die Art, der Umfang und die Umstände der zugrundliegenden Verarbeitung mit einzubeziehen.[3] Dieser risikobasierte Ansatz des Gesetzes lässt gewisse Abwägungen zu, bedeutet jedoch auch, dass im Zweifelsfall im Rahmen der Rechenschaftspflicht dargelegt werden muss, warum kein hohes Risiko vorlag.

Unverzügliche Meldepflicht als Auftragsverarbeiter

Sofern man Daten als Auftragsverarbeiter verarbeitet, ist man nicht von einer Meldepflicht gegenüber der Datenschutzaufsicht betroffen.[4] Die Meldepflicht muss nach Art. 32 Abs. 2 DSGVO unverzüglich, also ohne schuldhaftes Zögern, gegenüber dem Auftraggeber erfolgen. Die Meldepflicht gegenüber dem Auftraggeber umfasst alle objektiven Umstände – die Einschätzung, ob der Vorfall gegenüber der Aufsichtsbehörde gemeldet werden muss, obliegt dem Auftraggeber.[5] Nur der Auftraggeber als verantwortliche Stelle im Sinne des Art. 4 Abs. 7 DSGVO kann abschließend die oben genannte Abwägung vornehmen.

Meldung an die Aufsichtsbehörde

Sofern es sich um einen meldepflichtigen Vorfall handelt, gilt es, die Meldung an die Aufsichtsbehörde vorzubereiten.

Auch wenn die Aufsichtsbehörden der Länder teilweise unterschiedliche Meldeformulare zur Verfügung stellen, sind die Inhalte jedoch alle sehr ähnlich und orientieren sich am Art. 33 DSGVO. Folgende Risikoabwägungen müssen unter anderem berücksichtigt werden:

- Beschreibung der Art der Verletzung
- Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle
- Beschreibung der wahrscheinlichen Folgen der Verletzung
- Beschreibung der vorgeschlagenen Maßnahmen zur Behebung der Verletzung

Der letzte Punkt ist im Sinne der Schadensminimierung der relevanteste. Hier gilt es, gute Lösungen zu finden und der Aufsichtsbehörde plausibel darzulegen, wie die Auswirkungen der Datenschutzverletzung verringert werden.

Die vorläufige Meldung

Da eine fristgemäße Meldung nicht immer vollumfänglich möglich ist, sehen die Aufsichtsbehörden auch eine vorläufige Meldung vor. Im Rahmen der vorläufigen Meldung ist es möglich, die bekannten Tatsachen innerhalb der gesetzlichen Frist zu melden. Der vollständig aufgeklärte Sachverhalt kann im Anschluss nachgemeldet werden.

Dokumentation

Der Art. 33 Abs. 5 DSGVO beinhaltet auch eine Dokumentationspflicht. Diese orientiert sich am Umfang der Meldepflicht aus Art. 33 Abs. 3 DSGVO, sodass alle mit der Datenschutzverletzung im Zusammenhang stehenden Fakten, Auswirkungen und ergriffenen Abhilfemaßnahmen zu dokumentieren sind.[6]

Benachrichtigung der Betroffenen

Sofern man im Rahmen der Risikobewertung zu dem Ergebnis kommt, dass voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen besteht, sind diese ebenfalls unverzüglich zu benachrichtigen. Auf die Benachrichtigung kann jedoch verzichtet werden, sofern die Bedingungen des Art. 33 Abs. 3 DSGVO erfüllt sind. Hier gilt zu überprüfen, ob eine Benachrichtigung erfolgen muss.

Souverän.

Fazit

Eine Datenschutzverletzung lässt sich nie vollständig ausschließen. Anhand der oben genannten Kriterien können Sie sich jedoch in engem Austausch mit dem Datenschutzbeauftragten auf den Ernstfall vorbereiten. //

Daten-schutz-konform.

Fußnoten

1 Vgl. Piltz/Pradel ZD 2019, 152 für die genaue Berechnung der Frist.
2 Paal/Pauly/Martini DSGVO Art. 33 Rn. 22.
3 Paal/Pauly/Martini DSGVO Art. 33 Rn. 23.
4 Paal/Pauly/Martini, 2. Aufl. 2018, DSGVO Art. 33 Rn. 39.
5 Kühling/Buchner/Jandt, 2. Aufl. 2018, DSGVO Art. 33 Rn. 18.
6 Kühling/Buchner/Jandt, 2. Aufl. 2018, DSGVO Art. 33 Rn. 25.

DATATREE Akademie – Kompetenzen im Datenschutz

Weiterbildungseinrichtungen gibt's doch inzwischen wirklich genug. Für jede Zielgruppe, jedes Themenfeld und ja, auch jeden Geldbeutel gibt es das passende Angebot, oder?
Wieso also nun auch noch eine DATATREE Akademie? Weil gerade in den Bereichen Datenschutz und Informationssicherheit nach wie vor ein großer Bedarf besteht. Immer mehr Fragen tauchen auf und wollen beantwortet werden.

Text: Jörg Fecke

In der DATATREE Akademie geht es nicht einfach nur um die klassische Vermittlung von Wissen. Ja, auch hier werden Workshops zu verschiedensten datenschutzrelevanten Themen angeboten. Doch das ist nur ein kleiner Teil des Konzeptes. Darüber hinaus begründet die Akademie sich in dem, was eine Akademie sein soll: ein Ort des Austauschs. Hier treffen sich Menschen aus den verschiedensten Disziplinen, um gemeinsam Lösungen für aktuelle und zukünftige Aufgaben in den Bereichen Datenschutz und Informationssicherheit zu entwickeln.

Direkter Kontakt und Erfahrungsaustausch auf Augenhöhe

Regelmäßige Treffen wie etwa der Kaminabend oder die Initiative für Informationssicherheit im Gesundheitswesen bieten Teilnehmern die einmalige Chance, mit zahlreichen Fachleuten aus der Branche in den direkten Kontakt zu treten und runden das Seminarprogramm ab. Nach wie vor fallen vielen bei dem Wort Datenschutz Ungewissheit, Bürokratie und weitere negative Attribute ein. Das wollen wir ändern und bieten deshalb Seminare für den Neueinsteiger bis zum Profi an. Ein wichtiger Teil einer funktionierenden Datenschutzkultur in Unternehmen.

Mehrwert durch jahrzehntelange Branchenerfahrung

Die Dozenten und Gesprächspartner der DATATREE Akademie zeichnen sich durch hervorragende Expertise in ihren Themenfeldern aus. Unabhängig davon ob DSGVO, Sicherheitslücken in der IT-Infrastruktur, e-privacy, Lead-Auditorien, Datenschutz in Kirchen und Einrichtungen öffentlicher Träger: Wir haben in jedem Fall den richtigen Ansprechpartner. Unsere Mitglieder zeichnen sich nicht nur durch oft jahrzehntelange Branchenexpertise aus, sondern vor allen Dingen auch durch die Beteiligung an verschiedensten hochaktuellen Thematiken und Forschungsprojekten wie etwa der digitalen Patientenakte. Darüber hinaus agieren viele in der Lehre an renommierten Hochschulen wie etwa Prof. Thomas Jäschke, Dr. Olaf Metner und viele weitere.

Das Wissen aus der jahrelangen Beratung von Konzernen, Regierungen, Kommunen, aber auch Kleinbetrieben wird im Rahmen der DATATREE Akademie weitergetragen. Hier entsteht ein neuer Ort des Wissensaustausches. //

PROGRAMM

Das aktuelle Programm der DATATREE Akademie ist online unter:
www.datatree.eu/datatree-akademie/bauen-sie-ihr-kompetenzprofil-aus

NEWSLETTER

Über unseren kostenlosen Newsletter halten wir Sie nicht nur über die neuesten Angebote auf dem Laufenden. Regelmäßig geben wir Einschätzungen aus Expertensicht zu aktuellen Problemlagen. Anmeldung gerne auch per Mail an **kontakt@datatree.eu**

***zertifizieren*:** [amtlich] beglaubigen, bescheinigen, mit einem Zertifikat versehen – DUDEN

Zertifizierung – braucht das irgendwer oder kann das weg?

Text: Jörg Fecke

Zertifizierung, das ist die kleine Schwester des Zeugnisses und des Prüfsiegels! Gewinnt keine Beliebtheitswettbewerbe und ist dennoch für jeden unverzichtbar. Wir sind seit frühester Kindheit darauf gepolt, für alles eine Beurteilung zur erhalten und es wird mit fortschreitendem Alter immer so bleiben:
Seepferdchen, Bundesjugendspiele, allgemeine Hochschulreife, Führerschein, Promotion, Standesamt, Schwarzer Gürtel, Sportküstenschifferschein, die Liste lässt sich ewig weiterführen. Es gibt für alles ein Zertifikat! Dementsprechend freuen wir uns über Zeugnisse und Urkunden, der eine mehr, die andere weniger.

„Zertifizierung ist zweifellos sehr wichtig, aber sie bewirkt keine Produktqualität, wo sie nicht vorhanden ist. Zertifizierung ist kein Selbstzweck, aber ein ausgezeichnetes Instrument, Produktqualität zu sichern und zu verbessern.“

JOSEPH M. JURAN –
WEGBEREITER DES QUALITÄTSMANAGEMENTS UNTER ANDEREM BEI TOYOTA

Dabei ist der Sinn durchaus einleuchtend. Zertifikate und Zeugnisse schaffen Vertrauen, Standards und eröffnen neue Möglichkeiten. Ohne Zertifizierungen läuft heute gar nichts mehr. Sämtliche Branchen, von der Landwirtschaft über den industriellen Sektor bis zum Dienstleistungssektor, sind durch eine Vielzahl von Zertifizierungen geprägt. Dank der Zertifizierung können sich Autobauer auf Zulieferer von der anderen Seite des Planeten verlassen. Können wir ohne Bedenken beherzt in ein saftiges Steak beißen, ohne uns Sorgen um Gentechnik, Gammelfleisch und BSE zu machen – also in den meisten Fällen. Normen und Verordnungen sind aber nicht nur für die globalen Lieferketten von essenzieller Bedeutung. Produkte und Dienstleistungen erhalten ohne Zertifizierung auch in vielen Fällen keinen wettbewerbsfähigen Zugang zu lokalen Märkten.

Der Reiz einer Zertifizierung: Glaubwürdigkeit. Kaum eine Institution genießt in weiten Teilen der Bevölkerung ein so hohes Ansehen wie etwa die verschiedenen TÜVs. Die Technischen Überwachungsvereine sind inzwischen ein Synonym für Kontrolle, Transparenz und Sachkunde. Der gute Ruf hat sich längst global herumgesprochen, der Umsatz der verschiedenen Anbieter geht in die Milliarden. TÜV-geprüft ist ein wichtiges Qualitätsmerkmal.

Was Zertifizierungen nicht leisten: die Qualität steigern! Ein Produkt oder eine Dienstleistung müssen allerdings eine gewisse Qualität haben, sonst gibt es schlicht und ergreifend keine Zertifizierung. Einer der Hauptgründe, wieso eine Zertifizierung Sinn macht. Man verschafft sich eine bessere Ausgangslage.

Mit einer Zertifizierung holt man sich anfangs eine Menge Arbeit ins Haus. Es handelt sich dabei um einen Prozess, der nicht an einem Nachmittag abgearbeitet wird. Der Aufwand lohnt aber aus den genannten Gründen. In Bezug auf Datenschutz und die Informationssicherheit ist eine Zertifizierung allerdings gar nicht so einfach.

Dabei ist sie gerade in diesen Bereichen durchaus sinnvoll – schließlich handelt es sich um DatenSCHUTZ und InformationsSICHERHEIT.

Mit der ISO 27001 existiert zwar eine zertifizierbare Norm, diese beschränkt sich aber ausschließlich auf den Bereich Informationssicherheit. Die DSGVO sieht mit dem Art. 42 vor, dass auch für den Datenschutz eine Zertifizierung von den Mitgliedsstaaten ermöglicht wird. Im Moment bleibt es bei der Absichtsbekundung. Wie genau sich eine möglichst DSGVO-konforme Zertifizierung trotz aller Hindernisse gestalten lässt, erklärt Horst Wenning in seinem Artikel auf Seite 23.

Gerade in Bezug auf den Datenschutz ist seit der Einführung der DSGVO der Stellenwert in der öffentlichen Wahrnehmung sprunghaft gestiegen, die Umsetzung gelingt in vielen Bereichen nach wie vor nur mangelhaft. Das betrifft uns alle. Die Verarbeitung personenbezogener Daten hat in vergangenen Jahren enorm zugenommen. Ein Ende dieses Prozesses ist nicht absehbar. Im Gegenteil: Alle 18 Monate verdoppelt die Menschheit die Menge an Daten. Daher ist eine Instanz, die mit einem Siegel die Einhaltung der DSGVO bestätigt, überfällig. Genauso wichtig wie eine Hauptuntersuchung für die Verkehrstüchtigkeit Ihres Wagens ist eine Zertifizierung für Ihre Kalender-App, den Fitness-Tracker und vieles mehr. //

Es wird langsam eklig!

Wenn man hierzulande die Menschen nach Forbrukerrådet fragt, dann kommt in den meisten Fällen Achselzucken oder die Vermutung, dass es sich um einen Snack eines schwedischen Möbelverkäufers handelt. Hinter dem so schwer aussprechbaren Wort verbirgt sich der norwegische Verbraucherrat, eine Regierungsbehörde und Verbraucherschutzorganisation, die sich immerhin schon seit 1953 für Verbraucherbelange nicht nur der Norweger einsetzt.

Text: Jörg Fecke

Vor einigen Wochen hat es der Forbrukerrådet auch in zahlreiche internationale Medien geschafft. Wieso? Die Damen und Herren aus Oslo haben sich mit beliebten Apps auseinandergesetzt. Untersucht wurden zehn Android-Apps. Das Ergebnis überrascht dann doch: Daten wurden an mindestens 135 Drittdienste gesendet. Betroffen sind beliebte Dating-Apps wie Tinder und Grindr oder der Periodenzyklus-Tracker MyDays.

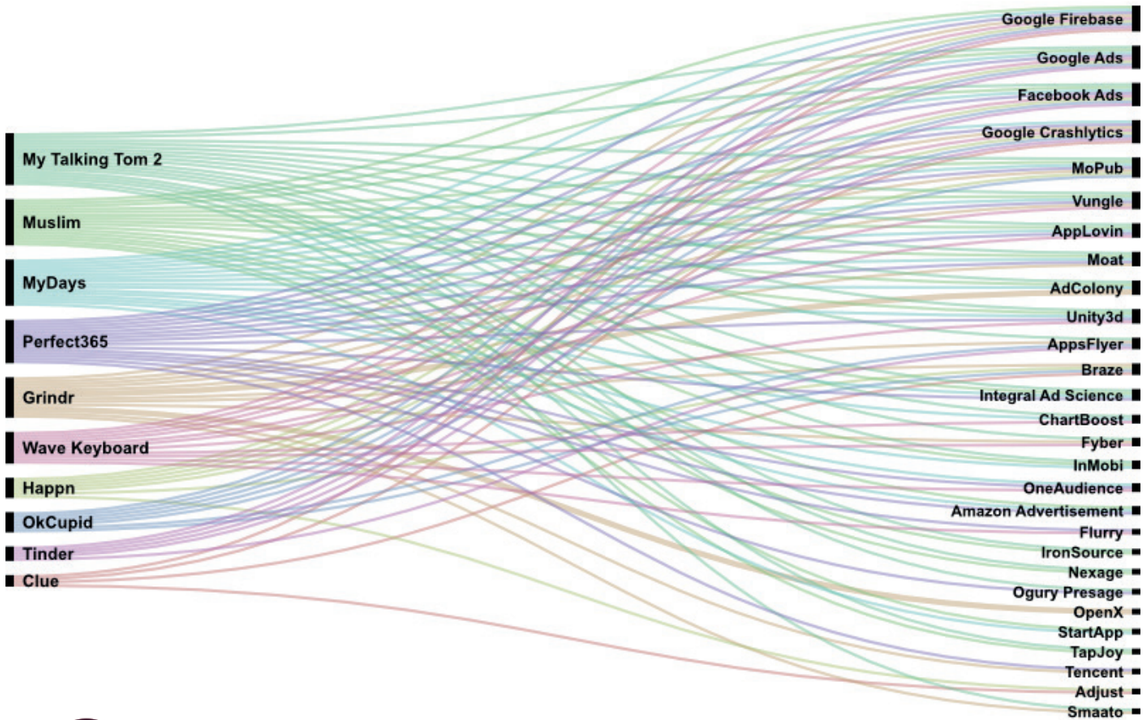
„Diese Geschäftspraktiken sind vollkommen außer Kontrolle geraten und verstoßen gegen europäisches Recht.“ – Finn Myrstad, norwegischer Verbraucherrat.

Der Nutzer hat keinen Überblick, was mit seinen Daten passiert. Von Aspekten wie Datensparsamkeit oder Privacy-by-Design ganz zu schweigen. Die norwegische Verbraucherberatung sieht hier systematische Verstöße gegen die DSGVO, die ja nun schon eine Weile Gültigkeit hat.

Während die App MyDays den Nutzerstandort verkauft, geht die App Grindr laut des Berichts noch einen Schritt weiter: Hier werden nicht nur Standortdaten weitergegeben, sondern auch sexuelle Vorlieben der Nutzer. Dass es sich hierbei um besonders schutzbedürftige Daten handelt, sollte jedem klar sein. Viel privater geht es nicht mehr. Besonders heikel, die App erfreut sich gerade in der Gay-, Trans- und Queer-Szene einer großen Beliebtheit. Deren sexuelle Vorlieben stehen nach wie vor in nicht wenigen Ländern unter Strafe, teilweise mit dem Tod.

Ironie des Schicksals: Eine EU-weit relativ unbekannte Einrichtung aus einem Land, das gar nicht Mitglied der Europäischen Union ist, findet, dass Millionen Anwender ein Recht auf die Durchsetzung der DSGVO haben. Nicht nur in Norwegen werden nun die Stimmen laut, dass den Usern eine DSGVO-konforme Nutzung zumindest ermöglicht werden muss. Langsam, aber sicher setzt sich die Erkenntnis durch, dass hier ein Prüfsiegel fehlt. //

Datenabfluss der getesteten Apps



Quelle: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf
Screenshot, alle Rechte vorbehalten Forbrukerrådet

Drum prüfe, wer sich ewig bindet

Der Wahn ist kurz, die Reu' ist lang.
Die Dienstleisterprüfung.

Friedrich Schillers Zitat aus dem Jahr 1799 hat auch 2020 noch eine große Bedeutung und zwar nicht ausschließlich auf Hochzeiten. Der Spruch passt auch hervorragend in andere Lebensbereiche – beispielsweise die Dienstleisterprüfung.

Text: Nina Richard

Warum Dienstleisterprüfungen?

Krankenhäuser, Krankenkassen und andere Einrichtungen des Gesundheitswesens sind aufgrund gesetzlicher, aufsichtsbehördlicher oder vertraglicher Anforderungen verpflichtet, ihre Auftragsverarbeiter auf die Einhaltung der datenschutzrechtlichen sowie sicherheitsrelevanten Anforderungen zu prüfen, die sogenannte AV-Prüfung.

Kalkulierbarer Aufwand?

Diese Prüfungen haben zur Folge, dass eine Zahl von ca. 120 Krankenkassen und 1800 Krankenhäusern sowie weitere Einrichtungen des Gesundheitswesens AV-Prüfungen bei ca. 250 bis 350 AV-Dienstleistern durchführen müssen. Dies wiederum bedeutet für die AV-Dienstleister, dass diese mit einer unkalkulierbaren Anzahl von AV-Prüfungen rechnen müssen. Zusätzliche Prüfungen von Aufsichtsbehörden sind auch noch möglich. Weder die prüfenden noch die zu prüfenden Einrichtungen verfügen über ausreichende personelle und zeitliche Ressourcen.

Organisation einer Prüfgemeinschaft

Mitglieder einer Prüfgemeinschaft werden jene Einrichtungen, die die Auftragsverarbeitung veranlassen oder zur Durchführung einer AV-Prüfung verpflichtet sind. Alle Mitglieder der Prüfgemeinschaft partizipieren von einer kompletten Organisationseinheit, die die vollständige Verwaltung und Koordination der Dienstleisterprüfungen durchführt. Darüber hinaus bietet eine Gemeinschaft weitere Vorteile wie den offenen Austausch über Herausforderungen und das Entwickeln gemeinsamer Lösungen.

Ablauf eines Dienstleister-Audits

- Datenschutz-Audits gemäß der Prüfung und Nachweispflicht der DSGVO
- Informationssicherheits-Audits gemäß ISO 27001/KRITIS

Bei einem Dienstleister-Audit (DL-Audit) handelt es sich um die Durchführung in der Organisation des Dienstleisters, die in der Regel nach folgenden Schritten erfolgt:

Vorbereitung

EINE GUTE VORBEREITUNG IST EXTREM WICHTIG

- Festlegung des Auditgegenstands und -umfangs, ggf. Festlegung eines Prüfschwerpunktes und Erstellung eines Auditplans
- Auswahl des zu auditierenden Dienstleisters oder der Dienstleistung nach den Vorgaben des Auftraggebers
- Informationsbeschaffung beim Dienstleister und Sichtung von Unterlagen (soweit für das Audit erforderlich)
- Auditplanung und Koordination mit dem Ansprechpartner des Dienstleisters und dem Auftraggeber
- Aufbereitung von Prüfkatalogen und Checklisten in Bezug auf den Auditgegenstand

Durchführung

JETZT WIRD ES ERNST

- Auditdurchführung in Form von Begehungen und stichprobenartiger Prüfung von Prozessen, Verfahren und Begutachtung der relevanten Dokumente zum Datenschutz und zur IT-Sicherheit
- Führen von Interviews mit den Mitarbeitern des Dienstleisters zu relevanten Prozessen, Verfahren, Vorgehensweisen und der entsprechenden Dokumentation

Nachbereitung

NACH DEM AUDIT IST VOR DEM AUDIT

- Zusammenfassung und Aufbereitung der Ergebnisse in einem Auditbericht für den Auftraggeber
- Bewertung möglicher Risiken und der datenschutzrechtlichen Eignung des Dienstleisters bzw. der Dienstleistung für den Auftraggeber

Die Organisation innerhalb einer Prüfgemeinschaft ist die kosteneffiziente Variante für Unternehmen, die zwangsläufig ihre Dienstleister prüfen müssen. //

Was Sie jetzt über Zertifikate wissen müssen

Die geänderten gesetzlichen Anforderungen im Bereich das Datenschutzes und der Informationssicherheit haben uns nicht zuletzt eine Fülle neuer Normen und Regelungen beschert. Dieser Artikel soll eine Übersicht über die relevanten Normen und Zertifizierungen geben.

Text: Horst Wenning

In vielen Bereichen stellen Zertifizierungen heute schon den Nachweis der erfolgreichen Umsetzung von gesetzlichen oder regulatorischen Anforderungen dar. So weisen z. B. Krankenhäuser die erfolgreiche Einführung eines Qualitätsmanagementsystems durch eine Zertifizierung nach ISO 9001 oder KTQ nach, andere Unternehmen wiederum weisen ihre Maßnahmen für die Informationssicherheit mittels einer Zertifizierung nach ISO 27001 oder IT-Grundschutz nach.

Wonach viele Unternehmen derzeit Ausschau halten, ist ein Zertifikat für die Umsetzung der DSGVO, um für Kunden und Interessenten einen anerkannten Nachweis zum Datenschutz zu erhalten.

Besondere Relevanz im Zusammenhang mit der DSGVO

Die DSGVO schenkt der Zertifizierung besondere Beachtung und behandelt sie im Verordnungstext: Art. 42 (Zertifizierung) und Art. 43 (Zertifizierungsstellen) legen die Basis für eine Datenschutzzertifizierung. Die Bedeutung einer künftigen Datenschutzzertifizierung wird deutlich, wenn man sich vor Augen führt, wo überall in der DSGVO das Stichwort Datenschutzzertifikate eine Erwähnung findet:

- Zur Auftragsverarbeitung im Art. 28 DSGVO: Geeignete Datenschutzzertifikate können herangezogen werden, um hinreichend zu garantieren, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

■ Bei der Datenübermittlung in Drittstaaten im Art. 46 DSGVO: Datenschutzzertifikate gehören zu den möglichen Garantien für ein angemessenes Datenschutzniveau, wenn es um die Rechtsgrundlage für die Datenübermittlung in einen Drittstaat geht.
■ Die generellen Bedingungen für die Verhängung von Bußgeldern im Art. 83 DSGVO: Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Höhe wird in jedem Einzelfall auch die Einhaltung von genehmigten Zertifizierungsverfahren nach Art. 42 DSGVO gebührend berücksichtigt. Mit anerkannten Datenschutzzertifikaten ließen sich somit die notwendigen Nachweise bei der Auftragsverarbeitung bzw. der Datenübermittlung in Drittstaaten erbringen. Bei der Ahndung einer Datenschutzverletzung könnten damit mögliche Bußgelder in der Höhe „positiv beeinflusst“ werden, also Bußgelder niedriger ausfallen oder sogar vollständig entfallen.

Welche Datenschutzzertifikate gibt es?

ISO/IEC 27701:2019-08 „Informationstechnik – Sicherheitsverfahren – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Datenschutzmanagement – Anforderungen und Leitfaden“: Die Internationale Organisation für Normung (ISO) hat mit der ISO 27701 eine Norm zum Nachweis der Einhaltung datenschutzrechtlicher Vorschriften auf der Basis der ISO 27001 als Norm der Informationssicherheit veröffentlicht.

Die Ähnlichkeit der Bezeichnung der beiden Normen ist nicht zufällig, da mit der ISO 27701 die ISO 27001 lediglich um Datenschutzaspekte erweitert wird. Zu einer erfolgreichen Zertifizierung nach ISO 27701 gehört damit die Umsetzung eines vollständigen ISMS mit der Wahl des relevanten Geltungsbereichs. In der ISO 27701 sind die Änderungen vor allem sprachlicher Natur. Statt von „Informationssicherheit“ ist nun die Rede von „Informationssicherheit und Datenschutz“. Des Weiteren enthält die Norm natürlich auch inhaltliche Erweiterungen. So wird bei der Betrachtung des Kontextes der Organisation ausdrücklich die Berücksichtigung der relevanten Datenschutzgesetze sowie die fortlaufende Betrachtung gerichtlicher Entscheidungen verlangt. Im Rahmen der Risikobeurteilung sind Aspekte der Verarbeitung von personenbezogenen Daten herausgehoben. ISO/IEC 27552 „Informationstechnik – Sicherheitsverfahren – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Datenschutzmanagement – Anforderungen und Leitfaden“ stellte die Entwurfsfassung der ISO 27701 dar.

ISO 27701 – das Datenschutzzertifikat?

Leider entspricht die ISO 27701 nicht dem gewünschten Datenschutzzertifikat. Im Art. 42 DSGVO wird die Einführung von DSGVO-Zertifizierungen vorgesehen. Diese sollen den Nachweis ermöglichen, dass bei den Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern die relevanten Anforderungen der DSGVO eingehalten werden. Im Art. 43 der DSGVO werden die einzuhaltenden Anforderungen an eine mögliche Zertifizierungsstelle beschrieben. Und hier liegt dann auch der Hund begraben: Der Art. 43 DSGVO fordert die Akkreditierung von Zertifizierungsstellen entsprechend der ISO 17065, die auf die Zertifizierung von Produkten und Prozessen ausgerichtet ist. Bei der ISO 27701 handelt es sich, wie oben beschrieben, um eine Erweiterung der ISO 27001. Damit stehen hier die Anforderungen an Managementsysteme im Mittelpunkt, deren Zertifizierung sich nach ISO 17021 richtet.

Zunächst ist die ISO/IEC 27001 nach wie vor die einzige zertifizierbare Norm der ISO 27000er-Reihe. Außerdem würde ein ISO-27701-Zertifikat nicht den aktuellen Anforderungen der DSGVO entsprechen. Dabei stellt dies eher ein formales Problem dar, da Managementsysteme im Kern auch prozessorientiert aufgebaut sind. Das bedeutet, dass eine Zertifizierung der Konformität zur ISO 27701 zurzeit höchstens indirekt erreicht werden könnte. Denkbar wäre hier z. B. die Nennung der ISO 27701 im Geltungsbereich des ISO-27001-Zertifikats nach entsprechender Überprüfung.

Somit ermöglicht auch die neue ISO 27701 nach aktuellem Stand noch keine „DSGVO-Zertifizierung“ gemäß Art. 42 DSGVO, aber sie bietet bereits heute die Möglichkeit, den Nachweis des DSGVO-konformen Umgangs mit personenbezogenen Daten zu führen. Durch die inhaltliche Verbindung zur ISO 27001 bedeutet die Einführung der ISO 27701 im Unternehmen keinen nennenswerten Mehraufwand. So kann bei der Umsetzung auf die bereits im Unternehmen vorhandenen Richtlinien, Prozesse und Dokumentationen zurückgegriffen werden, denn bei näherer Betrachtung zeigt sich außerdem, dass die ISO 27701 die Inhalte der DSGVO neu aufgreift und umstrukturiert. Sofern Unternehmen bereits die ISO 27001 umgesetzt haben und DSGVO-konform arbeiten, sollten die grundlegenden Anforderungen und viele der relevanten Maßnahmen bereits umgesetzt sein.

Fazit

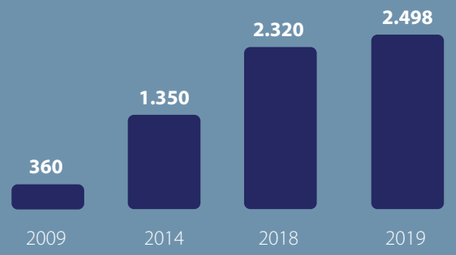
Mit der ISO 27701 wurden noch nicht alle Probleme auf einen Schlag gelöst, denn der Nachweis der Einhaltung des Datenschutzes gegenüber den Aufsichtsbehörden durch Vorlegen eines Zertifikats ist leider immer noch nicht möglich. Dennoch liefert die ISO 27701 einen wichtigen Beitrag für einen effektiveren Datenschutz und den interessierten Parteien einen Anhaltspunkt für die Anstrengungen eines Verantwortlichen oder Auftragsverarbeiters zur Umsetzung der Anforderungen der DSGVO. Schon heute kann die Zertifizierung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 mit einem Scope, der alle Bereiche umfasst, die personenbezogene Daten verarbeiten, die Basis für ein wirkungsvolles Datenschutz-Managementsystem (DMS) bieten. Umgekehrt stellen die in einem ISMS definierten Maßnahmen die technisch-organisatorischen Maßnahmen eines DMS dar. Es bleibt also spannend, ob die ISO 27701 eines Tages genauso relevant sein wird wie andere Normen, denn nach entsprechenden gesetzlichen Änderungen oder Ergänzungen der Normen wäre grundsätzlich ein DSGVO-Zertifikat auf der Basis der ISO 27701 vorstellbar. //

Haben wir die Kontrolle verloren?

Ich bin always on: vernetzt mit Menschen, die ich kenne oder denen, die ich gerne kennen würde. Von persönlichen Fangirl-Momenten bis hin zu Diskussionen über politische und gesellschaftliche Fragestellungen mit Menschen auf der anderen Seite der Welt, die ich niemals persönlich gesehen habe. Ich beschaffe mir Neuigkeiten und Informationen von jedem Platz auf der Erde, selektiert nach meinen Vorlieben, Wünschen und Interessen…von mir allein. Nie war ich so selbstbestimmt. Was für ein Trugschluss.

Text: Nina Richard

Erinnern Sie sich noch an Cambridge Analytica? Das US-amerikanische Datenanalyse-Unternehmen, dem ein nicht unerheblicher Beitrag zum Wahlsieg von Donald Trump nachgesagt wird. Was legal begann, nämlich im Namen der Wissenschaft, endete mit einem Verkauf von massenhaften Nutzerdaten. Nach Aufdeckung des Skandals durch Whistleblower Christopher Wylie hatten nicht nur Nutzer ein schlechtes Gefühl, zusätzlich verzeichneten die sozialen Medien einen enormen Vertrauensverlust. Auf die Facebook-Nutzerzahlen hatte das offensichtlich keinen großen Einfluss – die stiegen weiter kräftig.



Entwicklung der Anzahl der Facebook-Nutzer in Millionen.
(https://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/)

Vor einigen Wochen dann der nächste Skandal – das in den USA ansässige Unternehmen Clearview. Das Start-up entwickelte eine Gesichtserkennungssoftware. Allein das lässt sich schon aus Perspektive der Datenautonomie des Einzelnen kritisch betrachten. Das eigentliche Problem im Fall Clearview ist allerdings ein anderes. Die für die Polizei und private Unternehmen entwickelte Software bedient sich nämlich an Bildern der sozialen Netzwerke Twitter, Facebook und weiterer. Anders als der erste Blick vermuten lässt, ist das sogenannte Scraping, also das automatische Herunterladen von Bildern, die nicht als privat gekennzeichnet sind, nicht grundsätzlich illegal. Auf rechtlicher Ebene werden sich in Zukunft die Gerichte mit der Thematik beschäftigen.

Aber was lernen wir aus der Perspektive des praxisnahen Datenschutzes? Datenschützer warnen bereits seit Jahren vor der Speicherung massenhafter Ansammlungen von Daten, wie sie soziale Netzwerke vornehmen. Sie alle arbeiten beispielsweise mit automatischer Gesichtserkennung, die uns Nutzern als enormer Vorteil aufgeführt wird. Einen echten Mehrwert bietet sie allerdings nicht. Und wir? Wir geben irgendwelchen Firmen bereitwillig Daten in ihrer Reinform – Fotos von uns, unseren Freunden, Familien und Neugeborenen. Es erinnert fast an Opfergaben für unsere Götter – nur dass diese nicht mehr Allah oder Jehova heißen, sondern Facebook, Twitter oder Instagram.

Wie ist es nur soweit gekommen? 😱

Ja, natürlich kann man an dieser Stelle sowohl auf die lockeren Datenschutzanforderungen in den USA hinweisen als auch an die Eigenverantwortung eines jeden Einzelnen appellieren, der seine Daten schließlich freiwillig preisgibt. Wenn wir aber ehrlich sind, sind unsere modernen Systeme, die Art der Datenverarbeitung und auch die Einwilligung, die ich als Privatperson gebe, um ebendiese Technik nutzen zu können, völlig intransparent. Ein erheblicher Einschnitt in das Persönlichkeitsrecht jedes Einzelnen von uns und ein weiterer Schritt in Richtung Überwachung.

Gibt es überhaupt Alternativen?

Umso wichtiger ist die Verantwortung, die Datenverarbeiter tragen, denn jedes der Unternehmen, das Daten verarbeitet oder Software entwickelt, sich neuester Technologien bedient, hat eine Verantwortung. Und das Spannende ist: Datenschutzkonforme Lösungen sind möglich. Insbesondere in einem Land wie Deutschland, in dem wir die besten Voraussetzungen und das Know-how haben. Ich spreche an dieser Stelle nicht davon, dass wir Digitalisierung verhindern sollten – aber wir müssen die Technik, die wir bauen und einsetzen, datenschutzkonform entwickeln. Hier bedarf es Datenschützer, die die IT-Systeme verstehen, die Verarbeitung von Daten nicht behindern, aber datenschutzkonform umsetzen können. Also weg von rein wirtschaftlichen Interessen. Raus aus dem Datenrausch, hin zur Grundidee des Datenschutzes: dem Schutz des Einzelnen!

Doch wie, wenn nicht einmal mehr die Experten wissen, wie Anwendungen wie Twitter kontrollierbar sind? Stefan Brink, Landesdatenschutzbeauftragter aus Baden-Württemberg, kehrt Twitter den Rücken und empfiehlt dies auch anderen Unternehmen und Behörden. Sind wir bereit, diesen Preis zu zahlen?

🤔

Ablauf eines KRITIS-Audits nach ISO 27001

Ein Audit ist für jede Einrichtung eine Herausforderung, die nicht nur Ressourcen bindet, sondern auch einer hervorragenden Vorbereitung bedarf.

Text: Sascha Czech

Zunächst gilt, eine gute Vorbereitung ist das halbe Audit. Noch vor dem Pre-Audit ist unbedingt darauf zu achten, was allerdings eine Selbstverständlichkeit sein sollte, dass sämtliche Dokumente, Leitlinien, Richtlinien und Verfahrensanweisungen, die sich innerhalb des Informationssicherheits-Managementsystems (ISMS) befinden, ein aktuelles Revisionsdatum aufweisen, das Vieraugenprinzip bei der Freigabe einhalten und somit gültig sind. Diese Dokumente sind der Audit-Einstieg und somit von hoher Bedeutung. Beginnend mit dem sogenannten Scope, also dem Anwendungsbereich des ISMS, arbeitet der Auditor sich zunächst durch die Normkapitel A5 bis A18 und erwartet dabei natürlich die Einsicht in die zuvor genannten Dokumente. Dabei ist es wichtig, innerhalb der Dokumente eine Konsistenz nachzuweisen, zum einen dass entsprechende Richtlinien der Normkapitel den Zielzustand klar vorgeben, zum anderen dass entsprechende Verfahrensanweisungen den Weg zur Zielerreichung detailliert beschreiben und vorgeben. Dies ist dann zudem durch stichprobenartige Kontrollen, z. B. in den Dashboards einzelner Systeme, nachzuweisen.

Bereits vor dem Pre-Audit bedarf es der Optimierung von Dokumenten

Theorie-/Praxisabgleich

Durch den eigenen, internen Auditplan und die intern durchgeführten Audits macht der Auditor sich ein Bild davon, ob das eigene ISMS auch tatsächlich gelebt und dessen Anwendung intern auch überprüft wird. Die internen Audits der einzelnen Normkapitel sollten sich daher anhand eines internen Auditplans, welcher sich über nicht mehr als drei Jahre verteilen sollte, nachzuweisen. Sofern bereits bei einem internen Audit Abweichungen oder Nebenabweichungen festgestellt wurden, sind sowohl die entsprechenden Abweichungen als auch der Maßnahmenplan sowie dessen Umsetzung zu dokumentieren und nachzuhalten.

Zusammengefasst beginnt jedes Audit also mit dem Anwendungsbereich, über die Leitlinie, welche alle relevanten Schutzziele enthalten muss, über die den Normkapiteln zugeordneten Richtlinien und Verfahrensanweisungen. Dabei empfiehlt es sich, den Dokumentenstamm direkt nach den Normkapiteln aufzubauen und zu benennen, damit der Auditor sich zu jeder Zeit auch innerhalb des Dokumentenstamms zurechtfindet.

User-Change-management steht im Fokus

Nach dem Dokumentenstamm schaut sich jeder Auditor gerne das User- bzw. das User-Changemanagement an. Den Fokus hierbei legen die Auditoren auf ein nachvollziehbares Verfahren von der User-Anlage über die User-Änderung bis hin zur User-Deaktivierung.

„Warum wurde ein User angelegt, wer hat dies beantragt und was ihn dazu berechtigt?“ Dies sollte unbedingt lückenlos dokumentiert sein. Auch sollte es Vorlagen für Standardberechtigungen verschiedener Usergruppen geben, nicht nur innerhalb der Active Directory, sondern auch auf der Applikationsebene.

Als Nächstes liegt das Augenmerk in der Regel auf dem Changemanagement bzw. der Schnittstelle zwischen dem Changemanagement und der Informationssicherheit. Hierbei ist von großer Bedeutung, nicht nur entsprechende Richtlinien und Verfahrensanweisungen vorzulegen, sondern die tatsächliche und tägliche Anwendung gegenüber dem Auditor nachzuweisen. Dies kann beispielsweise durch eine Stellungnahme des Informationssicherheitsbeauftragten, welche dem Change beigefügt ist, nachgewiesen werden. Dabei sollten der Hintergrund des Changes, dessen Umsetzung und der Zielzustand beleuchtet werden.

Das Risikomanagement

Dabei ist es die Aufgabe des Informationssicherheitsbeauftragten, die Risiken daraus zu erkennen, in das Risikomanagement der Informationssicherheit aufzunehmen und mit konkreten Maßnahmen zu versehen. Hier wird der Auditor unter Garantie auch gerne etwas tiefer „graben“ und kann dabei durchaus auch Nachweise über mehrere Monate oder gar mehrere Jahre zurückliegend verlangen. Auch hier gilt daher: Je besser die gesamte Dokumentation innerhalb des Changemanagements gepflegt ist, desto leichter ist auch der Nachweis gegenüber dem Auditor.

Der Schwerpunkt der Prüfung liegt ganz klar im Risikomanagement der Informationssicherheit. Hierbei sollte unbedingt eine gute Richtlinie zum Risikomanagement die Basis der weiteren Bausteine bilden. Eine gute Richtlinie enthält klare und nachvollziehbare Vorgaben darüber, wie ein Risiko zu bewerten ist. Dies gilt insbesondere für die Faktoren „Eintritt“, „Auswirkung“, „Patientensicherheit“ und noch weitere. Es muss klar definiert sein, zu welchem Zeitpunkt oder besser gesagt bei welcher Auswirkung ein Faktor mit einer bestimmten, vordefinierten Wertigkeit belegt wird. Es ist genau vorzugeben, welche Kriterien zu erfüllen sind, um ein Restrisiko ohne Maßnahme zu akzeptieren und ab wann eine Reduktionsmaßnahme zwingend erforderlich ist. Die Umsetzung dieser Kriterien innerhalb der Richtlinie findet sich dann in der Risikomatrix wieder. Hier ist dem Auditor unbedingt nachzuweisen, dass zu jedem Normkapitel sowohl ein entsprechendes Risiko erfasst wurde als auch die entsprechende Einstufung der zuvor genannten Kriterien sowie der Umsetzungsplan der zugehörigen Maßnahme nachvollziehbar vorhanden sind. Auch die dokumentierte Maßnahme zur Risikoreduktion ist erneut nach vorangegangenem Schema dem Risikomanagement und einer Wirksamkeitsprobe zu unterziehen. Bedenken Sie: Das Risikomanagement der Informationssicherheit bezieht sich nicht alleine auf die IT-Bereiche, sondern erstreckt sich auf alle Bereiche des Unternehmens! Daher ist es wichtig, dass Verantwortlichkeiten, z. B. der Risikoeigentümer und der Risikoverantwortliche, für jedes einzelne Risiko klar definiert und benannt sind. Wichtig ist hierbei nicht, dass alle Maßnahmen zur Risikoreduktion abgeschlossen, sondern erkennbar in Bearbeitung sind.

Business Continuity Management

Der nächste wesentliche Punkt ist das Thema Business Continuity Management (BCM). Hierbei sind dem Auditor insbesondere das Notfallhandbuch sowie die vorhandenen und aktuellen Notfallpläne vorzulegen und nachzuweisen, dass entsprechende Notfallsituationen regelmäßig geübt und diese Übungen auch nachvollziehbar dokumentiert sind. Ein Schwerpunkt liegt hierbei auf dem Thema der Redundanzen für relevante Systeme. Wie schon bei den vorherigen Schwerpunkten erwähnt, ist das BCM keinesfalls ausschließlich auf den Bereich der Informationstechnik abzugrenzen. Vielmehr gilt hier das große Ganze, wie z. B. medizinische (Sub-)Systeme, Modalitäten, Bettentransport. Also alles, was für die Aufrechterhaltung des Versorgungsauftrags von Bedeutung ist. Dazu zählen durchaus auch das Heizsystem sowie die Klimaanlagen der Einrichtung.

> Richtlinie zum Risikomanagement dient als Basis

Als ebenso wichtig sei abschließend das Thema Datenschutz erwähnt. Ein aktuelles Datenschutzhandbuch ist für das Audit unerlässlich. Dabei sollte dies alle relevanten Bereiche des Datenschutzes beinhalten, so beispielsweise die Entsorgung von Datenträgern, der Umgang mit Systembenutzern, deren Bearbeitung und Löschung, sowie der Umgang mit Patientendaten, deren Auskunftsersuche und natürlich auch die Löschung von Patientendaten.

> Globaler Ansatz notwendig

Abschließend sei erwähnt, dass also alle Normkapitel der ISO/IEC 27001 zweifelsfrei erfüllt sein müssen. Die in diesem Artikel genannten Schwerpunkte geben einen ersten Anhaltspunkt für die Vorbereitung und den Ablauf eines Audits, sind jedoch aufgrund der Komplexität und Individualität jeder einzelnen Einrichtung nur oberflächlich beschrieben. //

DATATREE Akademie

VERANSTALTUNGSVORSCHAU
– 1. HALBJAHR –

Frühlingstreffen der Datenschutzbeauftragten

EXPERTEN- UND ARBEITSTREFFEN

Gute Datenschützer verfügen nicht nur über eine solide Know-how-Basis und Fachexpertise, sondern suchen auch den aktiven Austausch mit Fachkollegen und Experten aus anderen Schnittstellenbereichen. Nutzen Sie das Frühlingstreffen der Datenschützer, um in lockerer Atmosphäre über Trendthemen zu diskutieren und wertvolle Impulse für den eigenen Arbeitsalltag zu erhalten.

Termin: 2. April 2020, Dortmund

Kompaktseminar zum Datenschutzbeauftragten

LEHRGANG

Im Rahmen des Kompaktkurses zur/zum „Datenschutzbeauftragten“ erlangen die Teilnehmer in rund 30 Unterrichtsstunden das notwendige Expertenwissen, um als gesetzlich geforderte Datenschutzbeauftragte unternehmensintern wie -extern agieren zu können.

Termine: 4 x freitags ganztags 24. April., 08., 15. und 22. Mai 2020, Dortmund

Datenschutz in der Medizin – Update DSGVO 2020

FACHTAGUNG

Das Jahr 2019 war datenschutzrechtlich geprägt durch das Bemühen vieler Fachgremien und politisch verantwortlicher Stellen, die notwendige rechtliche Klarheit für die Anwendung der DSGVO zu schaffen. Dieser Prozess wird sich 2020 fortsetzen.

Termin: 4. Juni 2020, Wiesbaden

Treffen der Initiative für Informationssicherheit im Gesundheitswesen

EXPERTEN- UND ARBEITSTREFFEN

Der Zusammenschluss von Verantwortlichen der IT und Informationssicherheit, Geschäftsführern und Datenschutzbeauftragten arbeitet an der Sicherheit Deutschlands Krankenhäuser, sowie dem Schutz hoch sensibler Gesundheitsdaten. Es werden praxisnahe Handlungsempfehlungen und Tools für die Krankenhauslandschaft entwickelt und diskutiert. Wirken Sie aktiv mit!

4 x im Jahr, nächster Termin: 28. Mai 2020, Dortmund

Datenschutz-folgenabschätzung

WORKSHOP

Die Erstellung einer Datenschutzfolgenabschätzung kann immer dann notwendig werden, wenn sensible Daten verarbeitet werden. Die Bewertung solcher Verarbeitungsvorgänge kann sich, je nach Sachlage als sehr komplex erweisen. In diesem Workshop lernen Sie daher die wichtigsten Werkzeuge und Hilfestellung für den soliden Umgang mit Datenschutzfolgenabschätzungen kennen.

Termin: 21. April 2020, Dortmund

Ihr Kontakt zur DATATREE Akademie:

Nina Richard
Bereichsvorstand
Marketing & Kommunikation, Vertrieb
T 0231 54380333
nina.richard@datatree.eu

Julia Kleineberg
Assistenz
Marketing & Kommunikation
T 0231 543803330
julia.kleineberg@datatree.eu

www.datatree.eu

Impressum

ExperSite Ausgabe 01 2020 | ISSN-Print 2364-5636 | ISSN-Internet 2364-5644 | Herausgeber: DATATREE AG, Heubesstraße 10, 40597 Düsseldorf, T +49 211 93190-700, F +49 211 93190-799, office@datatree.eu, www.datatree.eu | Sitz der Gesellschaft: Düsseldorf | Registergericht: Amtsgericht Düsseldorf | Registernummer: HRB 66132 | Umsatzsteuer-Identifikationsnummer: DE 279402614 | Vorstand: Prof. Dr. Thomas Jäschke | Vorsitzender des Aufsichtsrates: Prof. Dr. Julius Reiter | Inhaltlich Verantwortlicher gemäß § 1 Abs. 4 TMG, § 55 Abs. 1 RStV und § 55 Abs. 2 RStV: Prof. Dr. Thomas Jäschke | Redaktionsleitung: Nina Richard | Design und Umsetzung: Julia Kleineberg, David Baertz | Druck: Druckerzeugnisse Gerbrunn | Auflage: 5.000 | Fotos: Titelbild: Shutterstock/toonsteb; S. 2: o.: unsplash, Agê Barros; Illustration: David Baertz; S. 3: Tom Schulte, Oberhausen; S. 4-6: André Druch; S. 7: Prof. Thomas Jäschke; S. 8: unsplash, Matthew Brodeur; S. 9: pixabay, coffeebeanworks; S. 11: unsplash, Agê Barros; S. 12-13: unsplash, Agê Barros; S. 14: Tom Schulte, Oberhausen; S. 15: Julia Kleineberg, Dortmund; S. 17-18: David Baertz, Herne; S. 19-20: mixkit.co, Kika Fuenzalida; S. 21: Shutterstock/kwest; S. 22: Shutterstock/ Nick Gheissari; S. 23-25: Shutterstock/toonsteb; S. 28-29: unsplash, Tim Gouw; S. 30, 31: unsplash, helloquence.