Ausgabe 01 2019

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Digitalisierung und Datenschutz
Ein Widerspruch?

Klinikalltag mit der DSGVO Wie läufts in der Praxis?

How-to Einwilligungen richtig gestalten

„DATEN sind das neue Öl."

John Boswell, Vizepräsident und Chefjustiziar des SAS Institute

Datenschutz langweilt Sie?

Das geht auch anders! Mit Praxisnähe, Professionalität und Leidenschaft. Wir zeigen Ihnen wie!

Trotz gesetzlicher Bestimmungen und Anforderungen muss Datenschutz kein langweiliges Thema sein. Mit unserem Ziel, Datenschutz lebbar zu gestalten, erfüllen wir die Bedürfnisse aller Interessenten – von der Geschäftsführung bis hin zum einzelnen Mitarbeiter: Datenschutz gesetzeskonform und spannend umgesetzt. Abgeleitet von der Betrachtung des Ist-Standes des Datenschutz-Niveaus entwickeln wir systematisch Ihre Datenschutz-Organisation und optimieren Ihre Prozesse. Unsere eigens hierfür entwickelte Software, sorgt für effiziente Prozesse und Zeitersparnis.

Datenschutz strukturiert aufbauen:

- ganzheitliches Datenschutz-Managementsystem
- modular aufgebaut
- gesetzliche Vorgaben erfüllen
- Datenschutz als Teil Ihrer Unternehmensphilosophie

DATATREE
YOUR COMPLIANCE PROVIDER

ISDSG
Institut für Sicherheit und Datenschutz im Gesundheitswesen

DATATREE AG • Heubesstraße 10 • 40597 Düsseldorf
T +49 211 93190-700 • F +49 211 93190-799
office@datatree.eu • www.datatree.eu

_ INHALT _

Daten sind mehr als moderne Rohstoffe_10

Erfolgreiche digitale Transformation setzt die richtige Architektur voraus_12

Die unterschiedlichen Welten der Datenschutzberatung_27

AKADEMIE 4

EDITORIAL 5

PROFILING
Spannende Persönlichkeiten zeigen, wofür ihr Herz schlägt 6

UNTERNEHMENSNEUIGKEITEN
Neujahrsempfang: „Das geht aus Datenschutzgründen nicht" 8

SCHWERPUNKT: DATENSCHUTZ & DIGITALISIERUNG
Daten als moderne Rohstoffe? 10

Erfolgreiche digitale Transformation setzt die richtige Architektur voraus 12

Fallstricke der DSGVO 16

DATENSCHUTZ UND INFORMATIONSSICHERHEIT
Datenschutz und Informationssicherheit messen und gestalten 24

DATENSCHUTZBEAUFTRAGTER
Die unterschiedlichen Welten der Datenschutzberatung 27

HOW-TO
Einwilligungserklärung richtig gestalten 28

VORSCHAU 31

Impressum

ExperSite Ausgabe 01 2019 | ISSN-Print 2364-5636 | ISSN-Internet 2364-5644 | **Herausgeber:** ISDSG – Ein Dienstleistungsbereich der DATATREE AG | 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 | **Editorial Design u. Umsetzung:** c74 gestaltung & design, C. Robrahn, Dortmund, www.c74.org | **Druck:** Druckerzeugnisse Gerbrunn | **Auflage:** 5.000 | **Fotos:** Titelbild: pixabay, A_Different_Perspective; S. 3 o.li. St. Marien Gesellschaft Siegen, Christian Stoffers; o. re.: pixabay, Free-Photos; pixabay, PixelAnarchy; S. 4: shutterstock, stas 11; S. 5: Tom Schulte, Oberhausen; S. 6: Julia Kleineberg, Dortmund; S. 8–9: Julia Kleineberg, Dortmund; S.10: St. Marien Gesellschaft Siegen, Christian Stoffers; S.12–13, 14: pixabay, Free-Photos; S. 16–23: unsplash jesse bowser, shutterstock,vs-148 ; S. 24–26: unsplash, harshal desai; S. 26: Prolytics GmbH; S. 27: pixabay, PixelAnarchy ; S. 28–29: 30, Nina Richard, Tom Schulte, Oberhausen; S. 30: Nina Richard; S. 31: unsplash, rik van der kroon, S. 32: pixabay, A_Different_Perspective

ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen | www.isdsg.de

Bauen Sie Ihr Kompetenzprofil aus!

Wir unterstützen Sie mit Praxisnähe, Fachexpertise und Leidenschaft.

SEMINAR

Datenschutz für Datenschützer

Bei der Tätigkeit des Datenschutzbeauftragten gilt es, vielseitige Kompetenzen vorzuweisen und sich stetig weiterzubilden. Mit diesem eintägigen Seminar erhalten Sie von praxiserfahrenen Experten konkrete Handlungsanleitungen zu Fachthemen.

26. MÄRZ, 03. JUNI, 10. SEPTEMBER, 11. NOVEMBER

DSB, INTERESSIERTE MIT BASISWISSEN IM DATENSCHUTZ

LEHRGANG

Kompaktseminar zum Datenschutzbeauftragten

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.

BEGINN JEWEILS IM MÄRZ UND SEPTEMBER, GANZTAGS, AN VIER AUFEINANDERFOLGENDEN FREITAGEN

ES SIND KEINE VORKENNTNISSE ERFORDERLICH.

KAMINABEND

DSB-Kaminabend

Die Kaminabende richten sich an Personen, die bereits an Seminaren der DATATREE-Akademie teilgenommen haben, sowie diejenigen, die sich den regelmäßigen Austausch zu Branchenthemen wünschen. Treffen Sie Fachkollegen und diskutieren Sie mit Experten in lockerer Atmosphäre.

21. MÄRZ UND 24. SEPTEMBER

DSB, INTERESSIERTE MIT BASISWISSEN IM DATENSCHUTZ

EXPERTENKREIS – ARBEITSTREFFEN

Treffen der Initiative für Informationssicherheit im Gesundheitswesen

Der Zusammenschluss von Verantwortlichen der IT und Informationssicherheit, Geschäftsführern und Datenschutzbeauftragten arbeitet an der Sicherheit von Deutschlands Krankenhäusern sowie dem Schutz hochsensibler Gesundheitsdaten. Gemeinsam leisten die Teilnehmer Aufklärungsarbeit im Bereich der Informationssicherheit. Es werden praxisnahe Handlungsempfehlungen und Tools für die Krankenhauslandschaft entwickelt und diskutiert. Wirken Sie aktiv mit!

09. APRIL, 02. JULI, 01. OKTOBER, 05.DEZEMBER

CISO, IT-LEITER, GESCHÄFTSFÜHRER, DATENSCHUTZBEAUFTRAGTE

DIE DATATREE-AKADEMIE

Als Ansprechpartner für Datenschutz und Informationssicherheit müssen Sie stets auf dem neusten Stand sein. Egal, ob es um Ihre Fachkompetenz innerhalb gesetzlicher Komponenten oder branchen- und fächerübergreifendes Know-how geht. Auch weiche Faktoren, wie Präsentationstechniken, werden mit uns abgedeckt. Wir statten Sie mit dem nötigen Werkzeug aus und bauen Ihr Kompetenzprofil weiter aus. Unsere Referenten und Dozenten sind Datenschutzbeauftragte, IT-Sicherheitsexperten und Fachanwälte für IT-Recht. Ihr direkter Kontakt zu uns: nina.richard@datatree.eu

Digitalisierung? Das geht aus Datenschutzsicht nicht!

Liebe Leserinnen,
liebe Leser,

der Begriff der Digitalisierung ist eines der klassischen Buzzwords unserer Zeit. Von vielen genutzt, von wenigen verstanden, nutzt es sich seit Jahren, charakterisiert durch mangelhafte Informationen, zunehmend ab.

Eines ist relativ schnell klar: Unternehmen, die komplett auf Digitalisierung verzichten, haben es schwer. Aber ist die Digitalisierung darüber hinaus überhaupt noch ein Wettbewerbsvorteil? In dieser Ausgabe betrachten wir die Digitalisierung aus der Perspektive der Informationssicherheit und des Datenschutzes. Getreu dem Motto: Fahren nur mit Führerschein, gilt es auch beim Umgang mit der Digitalisierung, das grundlegende Handwerkszeug zu beherrschen – sonst wird ein auf den ersten Blick harmloses Thema zu einer ungeahnt starken Waffe. Je unbedachter das eine Lager mit dem digitalen Gold umgeht, desto verbissener ist das andere Lager.

Innovative Projekte, digitale Lösungen, die Leben retten und Prozesse in Unternehmen wirtschaftlicher gestalten und die medizinische Forschung vorantreiben – zu viele Projekte werden gar nicht erst in Angriff genommen. Warum? „Das geht aus Datenschutzgründen nicht!“, sagt der Assistent zu seinem Chef, der zuletzt einen Artikel zu dem Thema gelesen hat. Damit ist das Thema dann gestorben. Zu Recht? Nein!!!

Ich kann es nicht mehr hören!

Während das eine Lager, Daten verbrennt, analysiert und unvorsichtig damit arbeitet, werden auf der anderen Seite grandiose Projektideen im Keim erstickt. Alles geht … Der Datenschutz ist kein Verhinderer … aber es geht nicht ohne Arbeit! Und dessen müssen wir uns bewusst sein.

Ihre Nina Richard
(Redaktionsleitung)

Über Klischees, die seiner Branche entgegengebracht werden, kann Henning Mertes nur lachen.

Ein Informationssicherheitsbeauftragter lässt tief blicken

Wir sind stolz auf unsere Mitarbeiter, die nicht nur interessante Persönlichkeiten sind, sondern mit Leidenschaft und Expertise unseren Kunden zur Seite stehen. Im Profiling-Interview gibt Henning Mertes Einblicke in seine Tätigkeiten im Bereich der Informationssicherheit.

Interview: Nina Richard

Du erfüllst auf den ersten Blick gar nicht das klassische Klischee. Ich dachte Fachleute im Bereich der Informationssicherheit sind Jungs in Kapuzenpullis?

Leider ein Klischee, das sich hartnäckig in allen Bereichen, die Informationstechnologien betreffen, hält. Kapuzenpullis und ähnliches waren noch nie mein Ding, und ich habe auch noch nie so etwas besessen. (Hält kurz inne) Obwohl doch damals zu meiner aktiven Handballzeit, da hatte ich Kapuzenjacken, in denen wir außerhalb der Halle trainiert haben.

Du bist seit ca. einem Jahr bei der DATATREE im Bereich der Informationssicherheit tätig. Warst du vorher schon in diesem Feld tätig?

Informationssicherheit hat mich als Thema schon immer sehr interessiert, seine schnelle Entwicklung bringt ständig neue Facetten mit sich. Das macht es einfach sehr spannend. Bereits vorher habe ich schon im Rahmen meiner freiberuflichen Beratertätigkeit versucht, Unternehmen in diesem Zusammenhang zu unterstützen, allerdings aufgrund meines anderen Schwerpunktes nicht auf dem hohen Niveau, wie es bei DATATREE der Fall ist.

Was zeichnet deine Tätigkeit besonders aus?

Ich freue mich, nun Teil der DATATREE-Familie sein zu dürfen. Der tägliche Umgang innerhalb des Teams findet auf einer sehr vertrauten

Ebene statt und sorgt im Büroalltag für eine lockere Atmosphäre. Und das tut, nebenbei bemerkt, der fachlichen Expertise meiner Kollegen keinen Abbruch. Jeder Mitarbeitende hat seine besonderen Qualifikationen und Fähigkeiten, die er konzentriert im Sinne des Kunden anwendet. Ich habe zum Glück den spannendsten Teil des Kuchens bekommen (zwinkert und lacht) und darf meine Erfahrung nutzen, um Informationssicherheit in den Unternehmen zu implementieren und das Bewusstsein für diese Thematik bei den Mitarbeitenden unserer Kunden zu wecken.

Henning, du bist auch als Dozent tätig. Welche Rolle spielt für dich die Lehre?

Die Lehre spielt eine sehr große Rolle für mich, schließlich bin ich in diesem Bereich seit mittlerweile fast 30 Jahren unterwegs. Auch in diesem Bereich darf man – genau wie im Bereich der Informationssicherheit – niemals stehen bleiben. Stillstand bedeutet für mich Rückschritt, weil die Welt sich weiterentwickelt. Außerdem hält mich der Kontakt mit den jungen Leuten auch selber jung.

Betrachten wir deine Beratertätigkeit nochmal etwas genauer. Was machst du bei einem typischen Kunden?

Wir implementieren in enger Zusammenarbeit und in Abstimmung mit den Kunden ein ISMS. Hierbei ist es spannend für mich zu sehen, wie unterschiedlich diese Thematik bei den unterschiedlichen Kunden gesehen wird. Daher ist unsere Beratung nach meinem Dafürhalten eminent wichtig, denn es hilft ja nichts, wenn man zig Richtlinien aufstellt und die Mitarbeitenden oder sogar die Geschäftsführung nicht dahinterstehen.

Und wenn der Auftrag abgeschlossen ist, ist das Unternehmen der Kunden sicher?

Sicherheit ist für mich nichts anderes als ein Missverhältnis und zwar zwischen Kosten und Ertrag. Man kann daher schon sagen, dass – wenn wir die entsprechenden Prozesse implementiert haben – ein Unternehmen schon ziemlich gut dasteht. Dadurch, dass wir uns in einem PDCA-Zyklus bewegen, sind wir eigentlich nie so richtig fertig. Man muss ja aus den jeweiligen Situationen immer wieder lernen, das Verbesserungspotenzial erkennen und auch entsprechend reagieren.

Aktuell sind die Medien wieder voll von Meldungen, bei denen sich Hacker Zugang zu Passwörtern und IT-Systemen verschafft haben. Was ist deines Erachtens das größte Problem von Unternehmen in Bezug auf die Informationssicherheit?

Ich sehe das größte Problem in der Arglosigkeit der Nutzer. Viele interessiert das Thema nicht wirklich, und dementsprechend wissen viele auch nicht, welche technischen Möglichkeiten existieren, um anderen zu schaden und gehen daher sorglos mit ihren Daten um. Wie sonst kann es sein, dass in Deutschland in den Top-10 der Kennwörter immer noch z. B. 123456 vorkommt? Wenn ein Kennwort erraten oder ermittelt wird und man als User dieses eine Kennwort bei allen möglichen Diensten nutzt, darf man sich wirklich nicht wundern, wenn man irgendwann einmal Schaden nimmt. In diesem Zusammenhang kann ich die Website https://haveibeenpwned.com empfehlen. Hier kann man checken, ob der E-Mail-Account betroffen ist.

Henning, vielen Dank, dass du die Zeit gefunden hast, dich mit mir zu treffen.

Dipl.-Kfm. Henning Mertes

Henning Mertes ist seit 1994 als Dozent für Datenbanken und Softwareentwicklung an unterschiedlichen Hochschulen und als IT-Berater tätig.

Im Rahmen seiner Tätigkeiten bei der DATATREE AG beschäftigt er sich mit Problemstellungen, die die Sicherheit von Unternehmensassets betreffen, und erarbeitet Prozesse unter Berücksichtigung bewährter Standards.

„Das geht aus Datenschutzgründen nicht“

Mit der DATATREE AG die richtige Datenschutzperspektive einnehmen

NEUJAHRSEMPFANG

Beim offiziellen Neujahrsempfang der DATATREE AG am 18. Januar 2019 trafen sich Kunden, Partner und Datenschutzinteressierte, um gemeinsam einen Blick in das Jahr der Informationssicherheit 2019 zu werfen – und in die neuen Geschäftsräume am Standort Dortmund. Rund 75 Teilnehmer erlebten ein abwechslungsreiches und modernes Veranstaltungskonzept.

Text: Nina Richard

Ende Dezember ist das Büro am Standort Dortmund vom Westfalendamm an die Märkische Straße in Dortmund gezogen. „Ein notwendiger und erfreulicher Schritt“, erklärt DATATREE-Vorstand Prof. Dr. Thomas Jäschke, „der dem positiv zu bewertenden Zuwachs personeller Ressourcen zu verdanken ist.“ Die neuen Räumlichkeiten erstrecken sich über zwei Etagen auf rund 600 Quadratmetern.

Liebe auf den zweiten Blick

Das Gebäude wirkt von außen eher wie ein unscheinbares Bürogebäude in Dortmund-Hörde und überrascht umso mehr, wenn man einen Blick hinein wirft. Offenes, klares Design mit gewollten Brüchen durch die Holzstützbalken des Altbaus verschafft den Räumlichkeiten einen Wohlfühlfaktor. Aber nicht nur die Besichtigung der neuen Räumlichkeiten war ein Highlight beim ersten Neujahrsempfang der DATATREE AG.

Vorstellung von Studienergebnissen: v. l. Michael Groß (Geschäftsführer prolytics), Emanuel Lungo (Projektleiter MaBIS), Frank Neumann (Bereichsvorstand Beratung und Vertrieb DATATREE AG).

Christine Thieme (Datenschutzberaterin DATATREE AG) über datenschutzkonforme Social-Media-Auftritte.

Zwiespältige Beziehung: Datenschutz und Digitalisierung

Eröffnet wurde die Veranstaltung von Prof. Dr. Thomas Jäschke, der in seiner Keynote „Das Jahr der Informationssicherheit; – gut gewappnet für die Herausforderungen des neuen Jahres“ einen Ausblick auf die kommenden Monate gab und auch einen Einblick in die Anfänge der DATATREE AG erlaubte: „Digitalisierung haben wir schon in den 90er-Jahren gemacht; da haben wir Scanner eingerichtet – das war damals Digitalisierung. Und heute, in Zeiten, in denen sich die Digitalisierung durch jegliche Geschäftsbereiche zieht, wird Digitalisierung, besser gesagt die damit gemeinte digitale Transformation, immer wieder in einen Gegensatz zum Datenschutz gebracht. Eine pauschale Aussage kann ich aber tatsächlich nicht mehr hören: Das geht aus Datenschutzgründen nicht!“ Unreflektierte Aussagen wie diese, so Jäschke, seien oft der Grund, weshalb innovative und wirtschaftlich bedeutende Digitalisierungsprojekte keine Chance bekämen: „Da behauptet jemand, der in die reale Umsetzung und in die Anforderungen des Datenschutzes keinen Einblick hat: Das geht aus Datenschutzgründen nicht. Und das ist dann plötzlich Fakt.“ In Wahrheit handele es sich aber häufig um Unwissen oder ein vorgeschobenes Argument, denn Datenschutz bedeute auch Aufwand innerhalb eines Projektes. Aufwand, der sich lohnt.

Abwechslungsreiches Programm

Anschließend konnten die Besucher aus verschiedenen Table Sessions wählen: Während das Thema softwarebasierte Managementsysteme von GAIMS-Geschäftsführer Dr. Tarek Gerdewal vorgestellt wurde, gab Emanuel Lungo, Projektleiter der prolytics GmbH, einen Einblick in erste Ergebnisse einer Benchmarkstudie zum Thema Informationssicherheit. Die DATATREE-Datenschutzberater Christine Thieme und Hanjo Tewes führten aus, wie sich die Teilnehmer datenschutzkonform im Social Web bewegen und wie sie Einwilligungserklärungen richtig gestalten.

Parallel dazu bestand für jeden Kunden die Möglichkeit, seinen Datenschutzberater zu treffen und sich mit ihm über Fachthemen auszutauschen. Nach einem Fingerfood-Büfett, mit Currywurst und Co. ging es in die zweite Session.

Die DATATREE AG

bietet seit 2011 eine umfassende Beratung in den Bereichen Compliance, Datenschutz und Informationssicherheit an. Sie berät und unterstützt öffentliche sowie nichtöffentliche Stellen bei der Einführung von Datenschutz-Managementsystemen sowie Managementsystemen für Informationssicherheit nach bewährten Standards, bei der Umsetzung konkreter Maßnahmen und Kontrollmechanismen. Zu den Kunden der DATATREE AG zählen kleine und mittelständische Unternehmen ebenso wie Großkonzerne – u. a. Krankenhäuser, medizinische Dienstleister, Behörden, IT-Dienstleister, Softwareentwickler und Wirtschaftsunternehmen.

Dr. Tarek Gerdewal (Geschäftsführer GAIMS) in seiner Table Session über softwaregestützte Datenschutz-Managementsysteme.

Auch in der Mittagspause gab es ausreichend Raum für angeregte Gespräche.

Das Marienheim Weidenau setzt den Roboter "Pepper" bereits im Alltag ein.

Daten als moderne Rohstoffe?

Bereits vor der CeBIT 2016 sagte Angela Merkel,
Daten seien die Rohstoffe des 21. Jahrhunderts.
Daten haben zweifellos einen hohen Wert, aber wie kommt es zu diesem?

Text: Henning Ullrich

In jedem Digitalisierungsprojekt sind Themen wir Datenschutz und Informationssicherheit unumgänglich und sollten zu den Grundpfeilern in jeder Planungsphase gehören. Nicht zu vergessen ist nämlich, dass im Rahmen von Big Data, insbesondere auch bei besonders schützenswerten Daten, die Begehrlichkeit und auch der Wert der erhobenen Daten, Datenströme und deren Analysen zunehmen. 100%ige Sicherheit existiert in der IT zwar nicht, diverse Datenhacks von Privatpersonen und Unternehmen zeigen aber immer wieder, wie notwendig Sicherheitsmaßnahmen sind. Dass Datenschutz und Informationssicherheit keinen Widerspruch zu innovativen Digitalisierungsstrategien bilden, zeigt die Praxis.

Big Data ist ein derzeit häufig genutzter Begriff. Einfach erklärt bedeutet er, durch die Analyse großer Datenmengen Informationen zu gewinnen. Am Beispiel der Krebsforschung lässt sich sehr schön zeigen, was damit gemeint ist. Es gibt eine Vielzahl von Therapien gegen Krebs. Diese sind aber oft nicht nur bei verschiedenen Arten von Krebs, sondern auch bei unterschiedlichen Menschen unterschiedlich wirksam. Häufig muss der behandelnde Arzt sich auf seine Erfahrung verlassen, um die richtige Therapie auszuwählen.

Erfolgreiche Therapien durch Big Data

Würden alle Therapieverläufe zusammen mit allen relevanten Daten in eine zentrale Datenbank eingetragen und ausgewertet, könnten Entscheidungen über die richtige Therapie aufgrund einer deutlich größeren Datenbasis getroffen werden, als nur der gesammelten Erfahrung des Arztes. Die Wahrscheinlichkeit, gleich zu Anfang die richtige Behandlungsmethode zu wählen nähme zu. Das hätte nicht nur steigende Überlebenschancen für die Patienten, sondern auch sinkende Kosten für das Gesundheitssystem zur Folge. Zukunftsmusik ist dies schon lange nicht mehr. Diesen Ansatz verfolgt das System Watson for oncology. Es basiert auf der KI Watson von IBM, befindet sich derzeit allerdings noch im Test. Watson soll sich einmal überall dort einsetzen lassen, wo Entscheidungen aufgrund großer Datenmengen getroffen werden müssen, andere Anwendungen sind beispielsweise die Recherche in juristischen Datenbanken und die Analyse von technischen Systemen, deren Komponenten aufgrund von Umwelteinflüssen frühzeitig ausfallen könnten und daher gewartet werden sollten. Aber auch Kliniken sind auf Digitalisierungskurs. Das Universitätsklinikum Essen hat als erstes Haus in ganz Deutschland seine komplette Labormedizin digitalisiert, wo ein spezialisiertes Team von Medizininformatikern und spezialisierten Ärzten Hand in Hand die Digitalisierung in der Medizin vorantreibt, indem es Labordaten auswertet, digitale Systeme entwickelt und sich mit der Optimierung der Automatisierung beschäftigt. Grundlage der Daten ist die Biobank Essen (WBE), die seit ihrer Einführung 2014 circa 300.000 Proben archiviert hat, mit dem Ziel, dass Ärzte eine bestmögliche Datengrundlage für ihre Therapieplanung erhalten (Jahresbericht 2016 Universitätsmedizin Essen). Auch für die Forschung ist die Datenbank wertvoll.

Unterstützung in der Pflege

Aber auch andere Bereiche wie die Pflegebranchen bleiben von der Digitalisierung nicht unberührt. Gestiegene Anforderungen an Pflegekräfte, der demografische Wandel und der damit einhergehende Fachkräftemangel machen dies unvermeidbar.

Die Unterstützung der Digitalisierung durch Regularien des Gesetzgebers wird in der Praxis kritisch gesehen. Unumstritten ist der Zuwachs der Pflegebedürftigen bis 2030 um etwa die Hälfte. Die Anzahl der Fachkräfte (Bertelsmann Themenreport Pflege 2030)[1] nimmt gleichwohl ab. Aber auch hier existieren viele Angebote und Testprogramme, die bei der Pflege helfen sollen: Unterstützung durch IT in der Dokumentation, wie in der Universitätsmedizin Essen, oder aber auch in Bezug auf die Bewohnerbetreuung, so wie es die St. Mariengesellschaft Siegen mit einem Forschungsprojekt der Universität Siegen tut: mit einem Pflegeroboter, der Mitarbeiter entlasten soll und Bewohner im Alltag unterstützt.

Die Bezeichnung „Roboter“ ist eigentlich falsch gewählt, wenn man in die großen Augen von Pepper blickt. Er hat Finger, einen Kopf und einen Körper, der stark an die menschliche Statur erinnert. Pepper unterhält die Senioren und Seniorinnen im Marienheim Weidenau, indem er mit ihnen musiziert, tanzt, Spiele spielt, Tai-Chi-Übungen ausführt oder sich mit ihnen unterhält. Roboter seien kein Ersatz für Pflegekräfte, so Dr. Christian Stoffers, Pressesprecher und Leiter des Zentralreferats Kommunikation & Marketing der Mariengesellschaft Siegen, sondern die Arbeit der Pflegekräfte sinnvoll ergänzen, diese somit entlasten und gleichzeitig die Betreuungsqualität für die Bewohner erhöhen.

1 https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/GP_Themenreport_Pflege_2030.pdf, S. 10

Erfolgreiche digitale Transformation setzt die richtige Architektur voraus

Dr. M. Tarek Gerdewal

ist Geschäftsführer der GAIMS GmbH. Er entwickelt und implementiert für namhafte Kunden Managementsysteme für Datenschutz und Informationssicherheit. Tarek Gerdewal unterrichtet an der FOM, Deutschlands größter privater Hochschule, unter anderem in Modulen, wie Big Data und IT-Infrastruktur, in Bachelor- und Master-Studiengängen.

Die digitale Transformation ist laut Fachpresse und diverser Studien in vollem Gange und in vielen Unternehmen bereits in der praktischen Umsetzung. Damit es nicht nur zu kurzfristigen Erfolgen kommt und Projekte aufgrund eines unüberschaubaren Umfangs und digitaler Überforderung der Mitarbeiter scheitern, wird eine solide Architektur benötigt: die Informationsarchitektur als Grundlage und Impulsgeber.

Text: Dr. M. Tarek Gerdewal

Als entscheidender Wettbewerbsfaktor und als Motor von weiteren Schlüsseltechnologien hilft die digitale Transformation den Unternehmen, weitere Potenziale auszuschöpfen und sich aktuellen und künftigen Herausforderungen flexibel entgegenzustellen (Digitale Agenda Bund und Bayern, 2018). Des Weiteren ermöglicht die digitale Transformation den Unternehmen, ihre eigene Position weiter auszubauen, neue Märkte zu erschließen und sogar den Gewinn zu steigern (Arbeit 4.0 in Brandenburg, 2018). Dabei nimmt die Informationstechnologie (IT) die Funktion eines sogenannten Enablers, also Befähigers, wahr.

Den richtigen Scope definieren

Laut einer empirischen Studie von Crisp Research aus Kassel, die in der „Computerwoche" vorgestellt wurde, werden IT-Abteilungen zunehmend bedeutungsvoller, um im Digitalisierungsprozess neue Ideen und Impulse zu geben. Allerdings wird die IT-Abteilung nicht als diejenige Abteilung im Unternehmen gesehen, deren Kernkompetenz die digitale Transformation sei (CW, 2015). Dies ist insofern nachvollziehbar, da die Transformation von Prozessen abteilungsübergreifend verwirklicht werden muss und dadurch eine enge Zusammenarbeit zwischen der IT und den Fachabteilungen erforderlich wird. Eine einseitige Umsetzung ist nicht zielführend und weniger hilfreich.

Mitarbeiter in den Fachabteilungen können sich leicht digital überfordert und nicht abgeholt fühlen, während sich Mitarbeiter in der Technik hingegen nicht verstanden fühlen. Die digitale Überforderung ist dabei in der Privatwirtschaft aufgrund des dort vorherrschenden Drucks höher als in der öffentlichen Verwaltung (Digitale Überforderung im Arbeitsalltag, 2016). Wie kann also ein Digitalisierungsprozess effektiv gestaltet werden?

Zur Vermeidung einer digitalen Überforderung ist es erforderlich, dass die Mitarbeiter im Unternehmen einen klaren Rahmen und Unterstützung im Digitalisierungsprozess erhalten. Der klare Rahmen definiert dabei den sogenannten Scope, um Schritt für Schritt die digitale Transformation umzusetzen. Die Unterstützung erhalten die Mitarbeiter dabei sowohl vom Management, als auch von den beteiligten Kollegen in der IT und in den Fachabteilungen. Gemeinsam gilt es, die Anforderungen an die digitale Transformation aufzunehmen, diese zu planen und zu prioriseren.

Grundlagen für die Digitale Transformation bilden

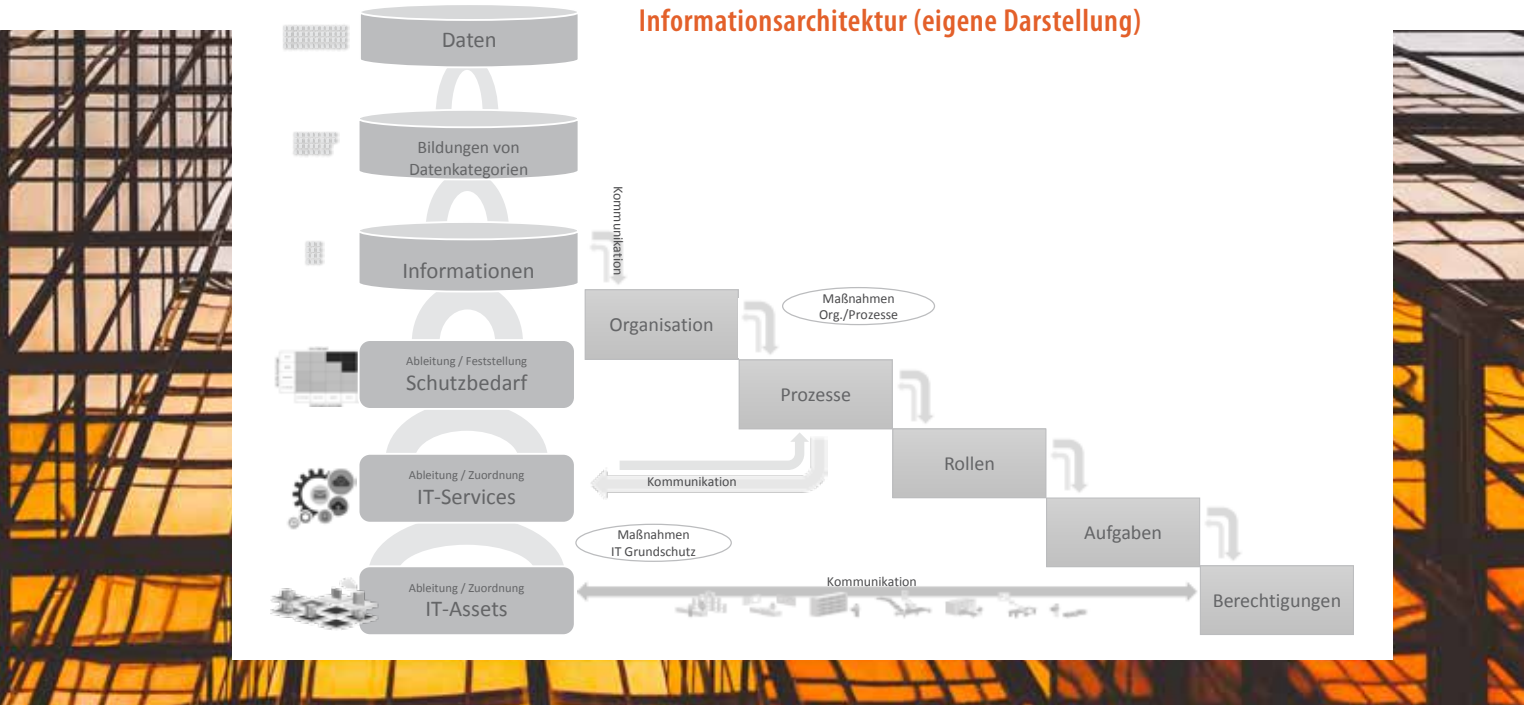
Auf dieser Grundlage kann die Art und Weise, also die Beschaffenheit oder Architektur, des Digitalisierungssystems bestimmt werden. Ist die Entscheidung für eine solide Architektur gefallen, kann nach deren Vorgaben eine schrittweise Umsetzung erfolgen.

Im Rahmen der IT sind hierbei verschiedene technische Architekturen zu berücksichtigen, wie beispielsweise die Systemarchitektur (Rechenzentrum, verteilte Entwicklungs-, Test- und Produktionsumgebungen etc.), die Softwarearchitektur (Frontend/Backend, Replikation, verteilte Persistierung, verteiltes Logging, Security etc.), die Netzwerkarchitektur (Skalierung, Replikation, Security etc.), die Schnittstellenarchitektur und nicht zuletzt die Cloudarchitektur. Bei der Softwareentwicklung ist noch zu beachten, ob eine monolithische Architektur oder eine Architektur auf Basis von Microservices aufgebaut wird. Weil Ersteres eine Menge an bekannten Nachteilen mit sich bringt (zum Beispiel steigt die Gesamtkomplexität der Anwendung mit der Zeit, steigende Aufwände und Kosten in der Skalierung, mit der Zeit abnehmende Releasezyklen und erhöhte Dauer für Wartungsarbeiten etc.), geht der Trend zu Microservices über (Microservices, 2019).

Bei Microservices handelt es sich um lose gekoppelte Services (ein Set von autarken Softwarefunktionen), die kooperieren und die über ihre eigene Datenbasis verfügen. Besondere Herausforderungen beim Aufbau von Microservices sind unter anderem die Projektkommunikation und -koordination zwischen den Entwicklerteams und den Fachabteilungen. Eine Einteilung der sogenannten Servicearchitektur kann nach Geschäftsprozessen (Neukundenanlage, Produktpflege, etc.), nach Fachgebieten/-abteilungen/-domänen oder nach einem sogenannten Domain-Driven-Design (Einkauf, Verkauf, Beschwerdemanagement, Logistik etc.) erfolgen. Welche technische Architektur ist also im Digitalisierungsprozess besonders zu berücksichtigen?

Informationsarchitekturen sind von besonderem Interesse

Im Kontext der digitalen Transformation und der engen Zusammenarbeit der verschiedenen Fachabteilungen ist jedoch die Informationsarchitektur von besonderem Interesse. Die Informationsarchitektur beschreibt dabei als eine Art Hilfsarchitektur nicht nur den Fluss der Daten und Informationen über Organisationseinheiten, Prozesse und IT-Komponenten hinweg, sondern gibt auch den nötigen Rahmen, den sogenannten Scope vor, in dem sich die digitale Transformation abspielt. Als Scope kann dabei wahlweise eine Abteilung (Organisationseinheit), ein relativ wichtiger Prozess oder ein kritisches IT-System (IT-Service) herangezogen werden.



Mithilfe der Zusammenhänge in der Informationsarchitektur ist es möglich, weitere Anforderungen abzuleiten und diese im Digitalisierungsprozess zu berücksichtigen. An zentraler Stelle ist der Schutzbedarf von Informationen verankert. Je nachdem, in welchen IT-Systemen schutzbedürftige Daten und Informationen verarbeitet werden, lässt sich der Schutzbedarf auf IT-Anwendungen und Prozesse vererben. Umgekehrt lässt sich der Schutzbedarf aber auch von kritischen Prozessen auf die IT-Systeme vererben.

Auf der Ebene der IT-Assets (IT-Infrastrukturkomponenten) werden die Maßnahmen des IT-Grundschutzes (BSI, 2019) umgesetzt, um eine grundlegende Informationssicherheit im Unternehmen zu gewährleisten. Hierbei können IT-Grundschutzprofile (branchen- oder nutzerkreisspezifische Schablonen für Informationssicherheit) hilfreich sein. Mit vordefinierten Profilen wird zum einen die Komplexität für die Anwender reduziert. Zum anderen können sich die Anwender ganz auf die Umsetzung der Maßnahmen und die Ermittlung von Defiziten konzentrieren (BSI-Magazin, 2018). Auf der Organisations- und Prozessebene sind je nach Anforderungen an die digitale Transformation Maßnahmen zur Optimierung von Prozessen und der Organisationsgestaltung notwendig. Für die Mitarbeiter im Unternehmen kann die Informationsarchitektur als eine Art Big Picture angesehen werden, mit dessen Hilfe die Zusammenhänge leichter erfasst, beschrieben und umgesetzt werden können. Auch die Einbindung von Dienstleistern, z. B. Cloudanbietern, in die Informationsarchitektur kann mit berücksichtigt werden, indem diese mit den eigenen Prozessen und Organisationseinheiten verknüpft werden. Auf Basis der Informationsarchitektur können somit weitere technische Anforderungen ermittelt und architektonisch umgesetzt werden.

Fazit

Die digitale Transformation ist bereits in vielen Unternehmen angelaufen und wird als entscheidender Wettbewerbsfaktor angesehen. Bei der Umsetzung der digitalen Transformation ist innerhalb der Unternehmen eine enge Zusammenarbeit und Kommunikation zwischen der IT und den Fachabteilungen notwendig. Aber auch zwischen kooperierenden Unternehmen muss eine enge Zusammenarbeit im Digitalisierungsprozess erfolgen. Die IT wird dabei in beiden Fällen als Enabler und Impulsgeber gesehen. Damit die Akteure, also die Mitarbeiter, im Digitalisierungsprozess keine digitale Überforderung erleiden und digitale Transformationsprojekte nicht scheitern, sollte man sich im Vorfeld Gedanken über den Rahmen der Projekte, die technischen Anforderungen und die Informationssicherheit machen. Als Grundlage hilft die Informationsarchitektur, aus der sich je nach Anforderungen weitere Abbildungsmöglichkeiten ableiten lassen.

Literatur

Arbeit 4.0 in Brandenburg (2018): Studie Arbeit 4.0 in Brandenburg, Internet: https://arbeit.wfbb.de/de/ZAB-Arbeit/Downloadcenter, abgerufen am 27.01.2019

BSI (2019): IT-Grundschutz, Internet: https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/itgrundschutz_node.html, abgerufen am 27.01.2019

BSI-Magazin (2018): Mit Sicherheit, Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2018_02.pdf?__blob=publicationFile&v=7, abgerufen am 27.01.2019

CW (2015): Computerwoche. Internet: https://www.computerwoche.de/a/it-abteilungen-sind-die-treiber-der-digitalisierung,3094502,2, abgerufen am: 27.01.2019

Digitale Agenda Bund und Bayern (2018): Internet: https://www.vbw-bayern.de/vbw/Aktionsfelder/Innovation-F-T/Forschung-und-Technologie/Digitale-Agenda-Bund-und-Bayern-3.jsp, abgerufen am 27.01.2019

Digitale Überforderung im Arbeitsalltag (2016): Internet: https://www.sopraseria.de/newsroom/publikationen/studie/digitale-ueberforderung-im-arbeitsalltag, abgerufen am 27.01.2019

Microservices (2019): Internet: http://microservices.io/patterns/microservices.html, abgerufen am 27.01.2019

UpDate!
Datenschutz by Esturias

FACHTAGUNG

Datenschutz in der Medizin – Update BDSG 2019

Das Jahr 2018 war datenschutzrechtlich geprägt durch das Bemühen vieler Fachgremien und politisch verantwortlicher Stellen, die notwendige rechtliche Klarheit zu schaffen für die Anwendung der DSGVO ab dem 25.5.2018. Dieser Prozess wird sich 2019 fortsetzen.

Termin: 07.05.2019
Ort: Mercure Hotel Wiesbaden City

Schirmherrschaft: Kassenärztliche Vereinigung Hessen (angefragt)
Für Fachanwälte IT-Recht und Medizinrecht findet § 15 FAO mit 6,0 Vortragsstunden Anwendung.
Für die ärztliche Fortbildung werden 8 Fortbildungspunkte anerkannt.

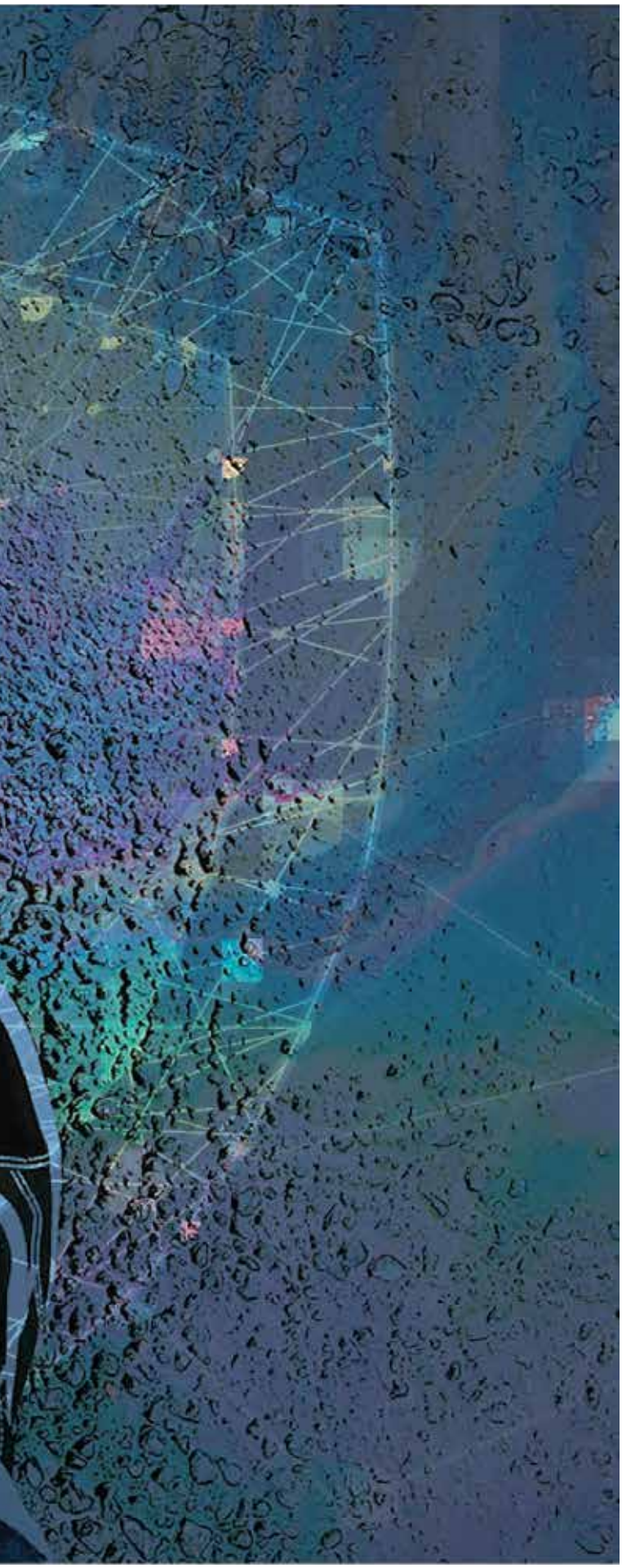
Geben Sie bei Ihrer Anmeldung den Rabattcode:
DAT_Update2019
an und erhalten Sie attraktive Vergünstigungen.

Weitere Informationen unter: www.esturias.de

Partner:
DATATREE YOUR COMPLIANCE PROVIDER
DVMD Der Fachverband für Dokumentation und Informationsmanagement in der Medizin
KHIT
digitales.hessen Intelligent. Vernetzt. Für Alle
Medizinrechtsanwälte e.V.

„Wenn Daten das neue Öl sind, dann ist Datenschutz der neue Umweltschutz.“

Jan Philipp Albrecht, ehemaliges MdEP, Landesminister in Schleswig-Holstein



Fallstricke der DSGVO

Das Recht auf Auskunft im Klinikalltag eines nichtöffentlichen Hauses

Die Datenschutzreform hat uns u. a. das umfassende Recht auf Auskunft gem. Art. 15 DSGVO beschert. Zwar ist dieses Recht nicht völlig neu, auch das BDSG-alt sah bereits ein Auskunftsrecht vor, was aber den Inhalt und die Anforderungen angeht, so ist dieses Recht nun wesentlich umfassender ausgestaltet als die Regelung im BDSG-alt.
Die DSGVO bietet den Betroffenen eine kaum zu begrenzende Möglichkeit der Datenauskunft. Auf der anderen Seite bietet dieses Recht keinerlei Schutz vor der missbräuchlichen Datenpreisgabe durch Firmen, die dies als Geschäftsmodell für sich entdeckt haben.

Text: Elke Stüve

Elke Stüve

ist Juristin und seit Mitte 2017 Konzern-Datenschutzbeauftragte der Asklepios Kliniken GmbH & Co. KGaA. Der Gesundheitskonzern Asklepios zählt zu den führenden privaten Betreibern von Krankenhäusern und Gesundheitseinrichtungen in Deutschland. Die Klinikgruppe steht für eine hoch qualifizierte Versorgung ihrer Patienten mit einem klaren Bekenntnis zu Qualität, Innovation und sozialer Verantwortung. Aktuell verfügt der Konzern bundesweit über rund 160 Gesundheitseinrichtungen und beschäftigt mehr als 47.000 Mitarbeiter.

Der Gesetzgeber hat bei der Reform des Datenschutzes leider den Zweck der Datenerhebung an keiner Stelle berücksichtigt. Personenbezogene Daten, die im Krankenhaus erhoben werden, dienen eben nicht als Zahlungsmittel für Dienste, die zur Verfügung gestellt werden, wie bei Facebook oder Google. Für das Krankenhaus sind Daten eben nicht „das neue Öl“.

Das Krankenhaus verarbeitet Daten, um den Patienten die bestmögliche Behandlung zu bieten, weil es gesetzlich dazu verpflichtet ist und ferner als Nachweis dafür, dass die Behandlung lege artis durchgeführt wurde.

Die Daten werden aber in keinem Fall als Zahlmittel missbraucht oder gar genutzt, um Menschen zu manipulieren.

Ein Recht auf Erhalt aller Informationen über die eigene Behandlung hatten Patienten schon vor der DSGVO durch § 630g BGB. Diese Regelung berücksichtigt das besondere Verhältnis zwischen Patienten und dem behandelnden Arzt. Darüber hinaus erhält der Patient durch Art. 13 DSGVO bei jeder Datenerhebung umfassende Informationen, die bereits weit über das hinausgehen, was die meisten Patienten interessiert, die in ein Krankenhaus kommen. So zeigte sich erst kürzlich eine Angehörige erzürnt, als wir ihr die umfassenden Datenschutzdokumente zum Behandlungsvertrag ihres Mannes zukommen ließen: „Mein Mann liegt im Koma und wird vermutlich sterben, und Sie haben keine anderen Probleme, als mir diese Datenschutzdokumente in die Hand zu drücken?“ Eine verständliche Reaktion, die Anlass zum Nachdenken darüber geben sollte, ob diese pauschalierte Informationsflut, zu der Krankenhäuser verpflichtet sind, tatsächlich sinnhaft ist. Hier zeigt sich mal wieder der Wahrheitsgehalt des Spruches „Gut gemeint ist nicht immer gut“.

Aber zurück zum Auskunftsrecht gem. Art. 15 DSGVO. Die vor dem 25.Mai 2018 erwartete Flut von Anfragen hielt sich zum Glück in Grenzen. Allerdings wurden fast alle Anfragen nicht gestellt, damit der Betroffene überprüfen kann, ob seine Daten rechtmäßig verarbeitet werden, sondern zur Geltendmachung als nicht voll umfänglich erfüllt angesehener Ansprüche oder als Reaktion auf abgelehnte Ansprüche. Ein anderer „Auskunftssuchender“ hat über 50 Kliniken angeschrieben und Auskunft verlangt, wohl in der Hoffnung, dass irgendwo die gesetzlichen Vorgaben nicht vollumfänglich berücksichtigt werden und er hieraus Kapital schlagen könne.

Und bei alledem darf nicht außer Acht gelassen werden, dass dieses Auskunftsrecht einen erheblichen Zeitaufwand für die Kliniken bedeutet.

Befindet sich eine Anfrage gem. Art. 15 DSGVO im Posteingang, so sind zunächst die drei Fragen zu klären, wer ist der Fragende, an wen ist die Frage gerichtet und was will der Fragende.

Mit diesen Fallstricken müssen Sie im Alltag rechnen:

Identitätsprüfung

Bereits hier tauchen die ersten Fallstricke auf. Art. 12 Abs. 6 DSGVO und Erwägungsgrund (EW) 64 sagen hierzu sinngemäß, begründete Zweifel an der Identität der betroffenen Person muss der Verantwortliche ausräumen. Es ist hierbei stets der Verhältnismäßigkeitsgrundsatz zu beachten. Bei Anfragen per E-Mail sollte grundsätzlich die Kopie des Personalausweises angefordert werden. Der Betroffene sollte bei der Anforderung darauf hingewiesen werden, dass er alle nicht zur Identifikation benötigten Merkmale schwärzen darf (z. B. Bild, Personalausweis-Nummer).

Wenn die Adresse auf dem Personalausweis und die bei der Klinik gespeicherte Adresse übereinstimmen, gelten damit eventuelle Zweifel als ausgeräumt. Die Daten können auf dem Postweg (auf einem Datenträger gespeichert) versandt werden. Bei Versand an die E-Mail-Adresse sollte vorher eine Risikoabwägung stattfinden. Der elektronische Weg ist zulässig, wenn keine Zweifel an der Korrektheit der E-Mail-Adresse bestehen (z. B. DE-Mail-Adresse). Je nach Risiko auch dann, wenn keine sensiblen Daten versendet werden (z. B. bei einer Negativauskunft).

Bei Zweifeln an der Identität kann z. B. eine amtliche Meldebescheinigung verlangt werden.

Ein Auskunftsersuchen darf auch telefonisch gestellt werden. Es ist in diesem Fall immer eine E-Mail-Adresse oder ggf. eine postalische Adresse und die Telefonnummer zu erfragen. Beim telefonischen Auskunftsersuchen ist zur Identifikation als erster Schritt immer die Übersendung einer Ausweiskopie zu verlangen. Dies sollte bereits schriftlich erfolgen.

Da die DSGVO nicht den Schutz Verstorbener umfasst, können keine Auskunftsersuchen gem. Art. 15 DSGVO für Verstorbene gestellt werden.

Verantwortlicher

Die genaue Bezeichnung des Verantwortlichen ist wichtig. Hier sollte beispielsweise nicht nur der Ort erfragt werden. Ansonsten kann es passieren, dass die Anfrage an den falschen Verantwortlichen weitergeleitet wird; z. B. an die Klinik statt an das MVZ. In diesem Fall müsste dann der Betroffene wiederum gem. Art. 13 DSGVO unverzüglich informiert werden, dass erstmals Daten über ihn bei einem Verantwortlichen verarbeitet wurden, dem die Daten irrtümlicherweise zugeleitet wurden.

Konkretes Auskunftsersuchen

Es muss klar sein, ob sich das Auskunftsersuchen auf Art. 15 DSGVO oder § 630g BGB gründet. Der Inhalt der Auskunft ist anders und gem. § 630g BGB können Kopierkosten verlangt werden. Des Weiteren sollte erfragt werden, in welcher rechtlichen Beziehung der Betroffene zum Verantwortlichen steht. Es erleichtert die Umsetzung erheblich, wenn im Voraus bekannt ist, ob der Betroffene als Patient, Mitarbeiter oder Bewerber mit dem Verantwortlichen in Kontakt steht bzw. stand.

Die Negativauskunft

Sind keine personenbezogenen Daten zu der Person gespeichert, so ist laut DSK dennoch eine Negativauskunft zu erteilen. Das Auskunftsverlangen und die erteilte Auskunft sollten zu Nachweiszwecken drei Jahre gespeichert werden. Gem. Art.13 DSGVO muss der Betroffene über die erstmalige Speicherung persönlicher Daten informiert werden. Dem Betroffenen ist daher Folgendes mitzuteilen: „…mit Ausnahme der personenbezogenen Daten, die Sie uns im Zusammenhang mit Ihrem Auskunftsersuchen mitgeteilt haben, haben wir keine Daten über Sie gespeichert. Bitte beachten Sie, dass wir Ihr Auskunftsersuchen und unsere Auskunft für Zwecke des Nachweises der ordnungsgemäßen Auskunft für einen Zeitraum von drei Jahren speichern.“

Ausschlussgründe

Sind diese Punkte geklärt, so sollten die gesetzlichen Ausnahmen von der Auskunftspflicht geprüft werden. In folgenden Fällen ist das Auskunftsrecht durch entgegenstehende Rechte eingeschränkt:

- § 27 BDSG: Die grundrechtlich gewährleistete Forschungs- und Wissenschaftsfreiheit wird gegenüber anderen Rechten privilegiert. In diese Privilegierung sind gem. EW 157 auch Big-Data-Anwendungen eingeschlossen („Verknüpfung von Informationen aus Registern"). Es muss zunächst die Erforderlichkeit der Datenverarbeitung für die Forschung geprüft werden. Darüber hinaus müssen die Forschungsvorhaben durch die Auskunft unmöglich oder ernsthaft beeinträchtigt werden. Beispiel: Verhaltensforschung, wenn die Auskunft das Verhalten des Betroffenen verändern würde.

- § 28 BDSG: Eine weitere Einschränkung des Auskunftsrechts besteht, wenn die Speicherung im Archiv im öffentlichen Interesse liegt. (EW 158 S. 2.) Private Stellen können betroffen sein, wenn diese im öffentlichen Interesse mit der Archivierung hoheitlich betraut sind.

- § 33 I Nr. 2 lit a, b BDSG : Zu prüfen ist weiterhin, ob das Auskunftsrecht eingeschränkt ist, weil dadurch die Geltendmachung gerichtlicher oder außergerichtlicher Ansprüche beeinträchtigt oder erschwert wird. Dies gilt allerdings nur, wenn die Daten bei Dritten erhoben wurden. Es muss immer eine Interessenabwägung stattfinden. Eine weitere Ausnahme liegt vor, wenn zivilrechtliche Vertragsdaten zur Prävention von Straftaten verarbeitet werden (Betrugspräventionsdateien) oder durch das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährdet ist bzw. Nachteile erleiden würde.

- § 34 I BDSG: Wenn die Speicherung nur aufgrund von Aufbewahrungspflichten oder zur Datensicherung bzw. Datenschutzkontrolle erfolgt, kann das Auskunftsrecht eingeschränkt sein. Wichtig ist hierbei § 34 Abs. 1 letzter Halbsatz BDSG: Die Auskunftserteilung muss einen unverhältnismäßigen Aufwand erfordern. Dies lässt sich bei modernen Suchfunktionalitäten schwierig begründen. Sollte die Norm einschlägig sein, so sind die Gründe zu dokumentieren und gegenüber dem Betroffenen zu begründen. Noch nicht geklärt ist die Vereinbarkeit dieser Regelung mit Art. 15 DSGVO. Die Ausnahme könnte EU-widrig sein.

Die Auskunft gem. Art. 15 Abs. 1 DSGVO

Nach der internen Recherche zu den Daten schließt sich die Auskunft gem. Art. 15 Abs. 1 DSGVO an. Das Ergebnis der Recherche ist dem Betroffenen in Form einer Liste der Datenkategorien zusammen mit dem Verarbeitungszweck, den Kategorien von Empfängern der Daten, Speicherdauer, Hinweis auf die Rechte aus den Artt. 16-18 DSGVO und dem Beschwerderecht mitzuteilen. Bei dritterhobenen Daten ist Auskunft über die Herkunft der Daten zu geben. Hierzu finden sich vielfältige Formulierungsvorschläge im Internet.

Bereitstellen der Kopie der Daten

Hat der Betroffene von seinem Recht gem. Art. 15 Abs. 3 DSGVO Gebrauch gemacht, so schließt sich eine weitere Prüfung, ob alle Daten auch in Kopie zur Verfügung gestellt werden dürfen und müssen, an. Die Datenkopie muss explizit verlangt werden. Sie muss nicht automatisch bei dem Auskunftsverlangen gem. Art. 15 DSGVO bereitgestellt werden.

Rechte und Freiheiten anderer Personen

Der Verweis in Art. 15 Abs. 4 DSGVO bezieht sich auf den Abs. 3, nicht auf Abs. 1b. Bei der Nennung des Absatz 1b handelt es sich um einen Redaktionsfehler.

Bei der Prüfung entgegenstehender Rechte Dritter ist immer eine Interessenabwägung mit dem Recht des Betroffenen auf Auskunft durchzuführen. Informationen zu anderen Personen dürfen geschwärzt werden, wenn ansonsten deren Rechte und Freiheiten beeinträchtigt würden.

Geheimhaltungspflicht

Als weitere Rechtsvorschrift schränkt § 29 Abs. 1 S. 2 BDSG das Auskunftsrecht ein. Die dort genannten „Informationen, die nach einer Rechtsvorschrift geheim zu halten sind“, wären beispielsweise die Auskunft über die leiblichen Eltern bei Adoptivkindern unter 16 Jahren (§ 63 Abs. 1 PStG).

§ 630g BGB

Bei Patientenakten gilt außerdem § 630g BGB: „soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung der Einsichtnahme ist zu begründen“. Eine pauschale Begründung ist an dieser Stelle nicht ausreichend. Die Begründung muss vom Arzt dokumentiert werden.

Übermittlung der Kopie der Daten

Bei Anforderung einer Kopie der Daten per E-Mail müssen die Daten in einem gängigen elektronischen Format (.pdf), aber nicht maschinenlesbar, zur Verfügung gestellt werden. Es ist unbedingt eine sichere Datenübermittlung (verschlüsselte E-Mail oder Zusendung eines verschlüsselten elektronischen Datenträgers und Zusendung des Entschlüsselungscodes zeitversetzt ebenfalls auf den Postweg) zu nutzen.

Bei einem postalischen Auskunftsersuchen ist die Kopie in Papierform als „Einschreiben Eigenhändig Rückschein“ zu versenden. Bei Papierdokumenten wird der verschlossene Postversand als ein hinreichend sicherer Übermittlungsweg auch für Gesundheitsdaten angesehen.

Auskunftsersuchen dürfen grundsätzlich nicht telefonisch beantwortet werden. In Ausnahmefällen muss allerdings die Auskunft mündlich erteilt werden, nämlich dann, wenn der Betroffene dies ausdrücklich verlangt. Für das Erteilen der mündlichen Auskunft ist ein Rückruf oder ein persönlicher Termin zu vereinbaren.

Die erste Datenkopie ist unentgeltlich zur Verfügung zu stellen (EW 59). Für jede weitere Kopie kann ein angemessenes Entgelt verlangt werden. Hat sich der Datenbestand allerdings signifikant verändert, muss in der Regel unentgeltlich eine neue Kopie zur Verfügung gestellt werden.

Wird die persönliche Abholung verlangt, so würde dies mit EW 59 kollidieren, da die persönliche Abholung mittelbar eine finanzielle Hürde bedeutet.

Da das Verhältnis von Art. 15 Abs. 3 DSGVO und 630g BGB noch nicht geklärt ist, müssen auch Patientenakten kostenfrei zur Verfügung gestellt werden. Dies kann aber mit dem Hinweis erfolgen, dass die Geltendmachung von Kostenerstattungsansprüchen für die Anfertigung der Kopie vorbehalten bleibt. Falls es in den nächsten Monaten hierzu eine gerichtliche Entscheidung gibt, können dann die Kosten ggf. nachträglich geltend gemacht werden.

Die Frist für dieses gesamte Verfahren beträgt einen Monat. Eine Fristverlängerung um zwei Monate ist möglich; die genannten Voraussetzungen der Komplexität oder einer hohen Anzahl von Anträgen müssen hierbei allerdings innerhalb eines Monats begründet werden. Die Fristberechnung richtet sich nach §§ 186 ff BGB. —

Datenschutz und Informationssicherheit messen und gestalten

Erste Ergebnisse der Benchmarkstudie MaBIS verfügbar

MaBIS ist die erste große Benchmarkstudie in deutschen Unternehmen, die nicht allein die Meinung der Experten für Datenschutz und Informationssicherheit in den Unternehmen einbezieht, sondern den Fokus auf die Einstellungen, den Kenntnisstand und das Verhalten aller Beschäftigten in diesen Unternehmen legt.

Text: Michael Groß und Emanuel Lungu

Experten für Informationssicherheit sind sich einig: Eine der größten Schwachstellen für Datenschutz und Informationssicherheit innerhalb eines Unternehmens ist der Faktor Mensch. Die zunehmende technische Komplexität im Arbeitsalltag sowie die immer höhere Professionalisierung von Cyberkriminalität machen die Behebung dieser Schwachstelle zu einem Thema, das derzeit jedes Unternehmen betrifft. Hinzu kommen gesetzliche Anforderungen und Bußgeldkataloge, die die Nichteinhaltung von Regularien für die betroffenen Unternehmen sehr kostspielig werden lassen können.

Ziel muss sein, dass Datenschutz und Informationssicherheit in den Unternehmen gelebt werden – nur so können Informations- und Verhaltensdefizite bei Mitarbeitern beseitigt werden.

An diesem Punkt setzt die Studie MaBIS an, denn sie beschäftigt sich mit der zentralen Frage: Ist Informationssicherheit im Unternehmen bei den Beschäftigten angekommen, und wie wird sie gelebt. Dabei verfolgt die Studie einen neuen Ansatz: Erstmalig liegt der Fokus der Befragung auf allen Mitarbeitern eines Unternehmens und nicht nur auf einzelnen Expertengruppen, und gibt so eine valide Beschreibung des Ist-Zustands der Informationssicherheit in den Unternehmen wieder.

Mit der kürzlich abgeschlossenen Benchmarkstudie liegt nun ein fundierter Branchenvergleich vor.

DIE STUDIE

METHODIK
Online-Access-Panel

STICHPROBE
n= 4000

BEFRAGUNGSZEITRAUM
November bis Dezember 2018

ZIELGRUPPE
Beschäftigte aus deutschen Unternehmen

BEFRAGUNG
Bewertung von 61 Aussagen zu unterschiedlichsten Aspekten der Informationssicherheit in den Unternehmen

DAS GESAMTERGEBNIS
Informationssicherheit ist aus Beschäftigtenperspektive in den Unternehmen (noch) nicht hinreichend gewährleistet

IM ÜBERBLICK

BEWERTUNGSAMPEL

ROT wenn mehr als 30 % der Antworten „eine negative Wirkung auf die Informationssicherheit haben".

GELB wenn 15 – 30 % der Antworten „eine negative Wirkung auf die Informationssicherheit haben".

GRÜN wenn weniger als 15 % der Antworten „eine negative Wirkung auf die Informationssicherheit haben".

Wie gut Informationssicherheit in den Unternehmen gewährleistet wird, erhebt die Studie mittels sechs Einflussfaktoren – persönliche Einstellung der Beschäftigten, Informationsstand im Arbeitsumfeld, Einfluss auf die tägliche Arbeit, Unternehmensimage zum Datenschutz und Aufklärung durch das Unternehmen – die ihrerseits von 61 Indikatoren bewertet werden. Die Ergebnisse werden am Ende für die einzelnen Indikatoren und Einflussfaktoren sowie für die daraus resultierende Informationssicherheit insgesamt ausgewiesen.

Grundsätzlich fühlten sich Befragte in Unternehmen mit einer Größe von 250 Beschäftigten und mehr besser im Bereich der Informationssicherheit aufgestellt als in kleineren Unternehmen.

In Anbetracht der Tatsache, dass Datenschutz und Informationssicherheit ein Thema sein sollte, das von jedem Beschäftigten im Unternehmen gelebt werden muss, ist es als besonders kritisch zu betrachten, dass sich in den Unternehmen ausschließlich das gehobene Management bezüglich Informationssicherheit fit fühlt. In allen anderen Unternehmensbereichen besteht eindeutig Nachbesserungsbedarf, insbesondere bei Hilfsarbeitskräften und Aushilfen.

Wie lebt Ihr Unternehmen Datenschutz und Informationssicherheit?

MaBIS können Sie auch in Ihrem Unternehmen durchführen. Dank der vorliegenden Benchmarkstudie haben Sie die Möglichkeit Ihre eigenen Ergebnisse mit Ergebnissen von Unternehmen aus Ihrer Branche zu vergleichen. Nutzen Sie MaBIS, um den Ist-Zustand innerhalb Ihres Unternehmens abzufragen, und so Schwachstellen und konkrete Handlungsbedarfe aufzudecken. So können Sie zielgenau Sensibilisierungs- und Aufklärungsmaßnahmen in Ihrem Unternehmen einleiten. Zudem erhalten Sie mit dem Ergebnis Ihrer Mitarbeiterbefragung Nachweise und Argumente bei Prüfungen und rechtlichen Angriffen. Auf Wunsch können unternehmensinterne Fragestellungen berücksichtigt werden. Bei einer regelmäßigen Durchführung der Mitarbeiterbefragung können Sie konkret die Erfolge Ihrer eingeleiteten Maßnahmen messen.

Gesamterfüllungsgrad des Themas Informationssicherheit bei den Beschäftigten

Differenziert nach Unternehmensgröße	Ampelwert
Gesamt	🟡
1 bis 9 Beschäftigte	🟡
10 bis 49 Beschäftigte	🟡
50 bis 249 Beschäftigte	🟡
250 und mehr Beschäftigte	🟢

Ausschließlich in großen Unternehmen fühlen sich die Beschäftigten hinreichend informiert.

Differenziert nach Position	Ampelwert
Gesamt	🟡
Gehobenes Management	🟢
Mittleres Management	🟡
Sachbearbeiter/Referentenposition	🟡
Facharbeiter/Vorarbeiter	🟡
(angelernter) Arbeiter	🟡
Hilfsarbeitskraft/Aushilfe	🔴
Sonstige	🟡

Lediglich das gehobene Management hält sich bei diesem Thema für gut aufgestellt.

Michael Groß
Geschäftsführer prolytics

Emanuel Lungu
Projektleiter MaBIS

Über prolytics

Prolytics ist ein Full-Service-Marktforschungsdienstleister. Gegründet im Jahr 1995, führt prolytics quantitative und qualitative Studien im Rahmen der Marktforschung sowie der empirischen Sozialforschung durch.

Die unterschiedlichen Welten der Datenschutzberatung

Gesetzliche Voraussetzungen für die Ausbildung als Datenschutzbeauftragte gibt es wenige. Zwar gibt die DSGVO einen groben Rahmen vor, der Auslegungsspielraum bleibt groß, wie auch die Spannbreite innerhalb der Beratungsqualität in der Praxis. Lassen Sie es uns doch einfach mal besser machen.

Text: Nina Richard

Ich bin eingeladen. Es trifft sich eine Datenschutz-Initiative. Man möchte uns als Mitglied für das Netzwerk gewinnen. Bei ein paar tausend Euro Mitgliedsbeitrag möchte ich mir vorab ein Bild der Veranstaltung machen. Der Veranstalter hat nicht gegeizt. Veranstaltungsort ist ein renommiertes Hotel in einer deutschen Großstadt. Ich freue mich auf den Expertenkreis. Auch das Programm ist vielversprechend. Die Netzwerkvertreter machen einen kompetenten und praxisnahen Eindruck. Relativ schnell wird mir allerdings klar: 90 % der Anwesenden sind Juristen. Grundsätzlich sind die Ansätze der Referenten fundiert und praxisnah. In dem Teilnehmerkreis, und das lässt mich an der Veranstaltung zweifeln, entwickelt sich aus einer durchaus spannenden und gerechtfertigten Diskussion über das Thema Veranstaltungsfotografie und -nutzung unter Berücksichtigung von DSGVO und TMG … eine Diskussion welche Kamera ein Fotograf denn nun nutzen müsse, damit es sich nicht um eine automatisierte Datenerhebung handelt und wie denn nun der Datenschutz beim Hausverein erfolgen soll, und welche Einwilligungen der Mitglieder bei der Sportveranstaltung XY notwendig seien.

Das ist der Zeitpunkt, an dem ich keine Lust mehr habe. Kein Experte, der die Anwesenden auf den Boden der Tatsachen zurückholt … es geht ausschließlich um die formelle Enthaftung. In mir macht sich das Gefühl breit, dass sich viele der dort Anwesenden an praxisfernen, unbedeutenden Details festkrallen. Verstehen Sie mich nicht falsch: Das Auslegen und das Anwenden der Datenschutzgesetze, sollten die Basis eines jeden guten Datenschutzbeauftragten sein … aber doch bitte nicht die Praxis vergessen. Meines Erachtens hat unser Berufszweig ein großes Problem, das genau hier, während ich in dieser Veranstaltung sitze, deutlich wird. Ein Großteil der Datenschutzbeauftragten vergisst den Alltag der Personen, die datenschutzkonform arbeiten müssen: Die Nicht-Juristen, die Nicht-Technikaffinen, die Menschen, die Datenschutz sowieso schon für realitätsfern halten. Genau das sind die Menschen, die wir in der Berater-Praxis, aber doch abholen müssen. Deshalb hier ein paar Tipps, die helfen, als Datenschutzbeauftragter zu glänzen:

1. Nehmen Sie andere Perspektiven ein.

Egal, ob Sie Jurist oder IT'ler sind, blicken Sie über den Tellerrand und bauen Ihr Fachwissen auf anderen Gebieten aus.

Jede Branche hat ihre schwarzen Schafe.

Sie müssen nicht alles können, aber Sie sollten ein Gefühl für andere Bereiche bekommen. Nur so schaffen Sie es, Datenschutzthematiken sinnvoll zu bewerten.

2. Bauen Sie ein Kompetenzteam um sich herum auf.

Gut aufgestellte Unternehmen schaffen Kompetenzteams, die es ermöglichen, Herausforderungen unternehmensweit zu diskutieren und zu lösen. Ihr Unternehmen ist noch nicht so weit? Ergreifen Sie die Initiative und bringen die Unternehmenskommunikation, die IT, Personal und Vertreter der anderen Fachabteilungen gemeinsam an einen Tisch.

3. Das geht aus Datenschutzgründen nicht.

Streichen Sie diesen Satz von nun an aus Ihrem Wortschatz. Sehen Sie sich als Möglichmacher, nicht als Verhinderer.

4. Schaffen Sie eine positive Fehlerkultur.

Erwischen Sie sich selbst manchmal dabei, wie Sie mit erhobenem Zeigefinger durch das Unternehmen laufen und Ihren Kollegen aufzeigen, was sie aus Datenschutzsicht zu unterlassen haben? Drehen Sie den Spieß doch einfach mal um und belohnen die Kollegen, die vorbildlichen Datenschutz leben. Wie wäre es z. B. mit einem internen Datenschutz-Wettkampf um die Trophäe der sichersten Abteilung?

Einwilligungserklärung richtig gestalten

Im Datenschutzrecht spricht man bezüglich der Verwendung von personenbezogenen Daten von einem Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass die Nutzung, Verarbeitung oder Speicherung von personenbezogenen Daten grundsätzlich verboten ist und nur erfolgen darf, sofern eine Rechtsgrundlage vorliegt. Eine der häufigsten Rechtsgrundlagen in der Praxis ist die Einwilligung (Art. 6 Abs. 1 a DSGVO).

Text: Hanjo Tewes

Die Grundidee der Einwilligung

Die Einwilligung beruht auf der Idee, dass jede Person über ihre eigenen personenbezogenen Daten frei verfügen kann. Dies bedeutet, dass neben der Möglichkeit, die Verwendung der personenbezogenen Daten zu untersagen auch die Möglichkeit besteht, die Verwendung zuzulassen. Wenn die betroffene Person einwilligt, spricht im Regelfall nichts gegen die Verwendung der personenbezogenen Daten, sofern die Einwilligung rechtmäßig war.

Welche Voraussetzungen der Gesetzgeber grundsätzlich an eine wirksame Einwilligung stellt, soll im Folgenden erläutert werden. Hierbei ist jedoch anzumerken, dass es sich um eine allgemeine Übersicht handelt, welche als Orientierungshilfe dienen kann, die jedoch bei jedem Einzelfall gesondert überprüft bzw. angepasst werden sollte. Eine besondere Vorsicht ist in Berufsfeldern mit besonderen Vertrauensstellungen (u. a. medizinische, soziale und juristische Berufe) sowie bei Einwilligungen von Minderjährigen geboten.

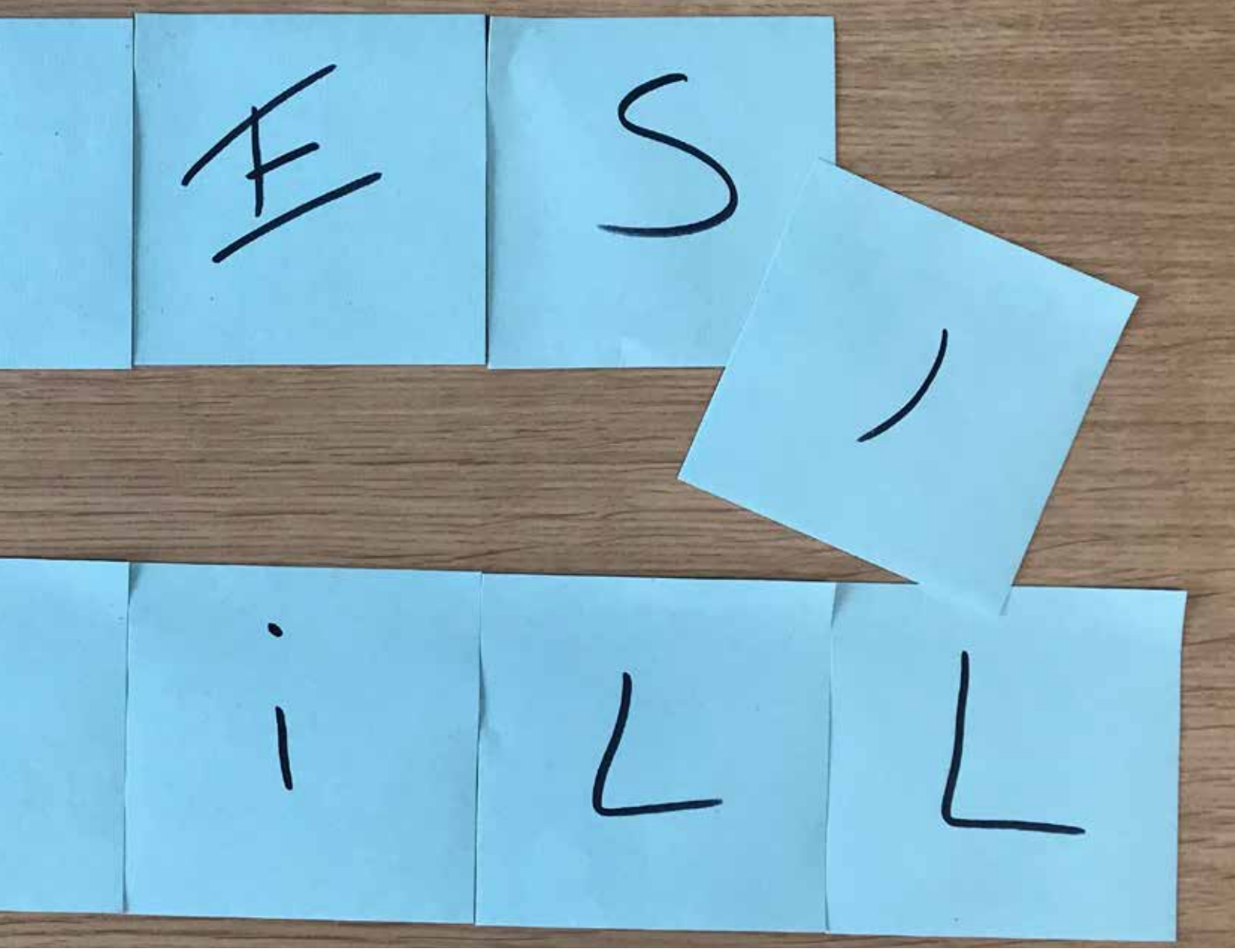
Form der Einwilligung

Das Einholen einer Einwilligung unterliegt keinen Formerfordernissen. Dies bedeutet, dass es grundsätzlich möglich ist, eine formlose Einwilligung einzuholen. Jedoch besteht bei einer formlosen Einwilligung eine Problematik im Rahmen der Rechtssicherheit. Nach Art. 7 Abs. 1 DSGVO muss die datenverarbeitende Stelle nach Art. 4 Abs. 7 DSGVO nachweisen, dass die Einwilligung erteilt wurde.[1] Dies ist Ausdruck der in Art. 5 Abs. 2 DSGVO normierten Rechenschaftspflicht.[2]

Aus diesem Grund sollte eine Einwilligung immer in Schriftform (per Hand unterschrieben) oder in Textform (z. B. per E-Mail) erteilt werden bzw. der Prozess der Einwilligung gut dokumentiert werden. So kann sichergestellt werden, dass auch nach längerer Zeit noch eindeutig nachweisbar ist, dass eine wirksame Einwilligung vorlag.

Wichtig ist, dass eine aktive Zustimmung für die Verwendung der personenbezogenen Daten vorliegt. Die bisher teilweise praktizierte Praxis der Einwilligung, sofern kein Widerspruch erklärt wurde (sog. Opt-Out-Einwilligung), ist im Rahmen der DSGVO nicht rechtmäßig.[3]

1 Kühling/Buchner/Buchner/Kühling, 2. Aufl. 2018, DS-GVO Art. 7 Rn. 27.
2 BeckOK Datenschutzrecht/Stemmer, 26. Ed. 1.5.2018, DS-GVO Art. 7 Rn. 86.
3 Kühling/Buchner/Buchner/Kühling, 2. Aufl. 2018, DS-GVO Art. 7 Rn. 26.



Bestimmtheit und Transparenz

Innerhalb der Einwilligung muss der Grundsatz der Bestimmtheit eingehalten werden. Dies bedeutet, dass vor der Erteilung der Einwilligung bereits festgelegt sein muss, wofür die personenbezogenen Daten verarbeitet werden.

Der Grundsatz der Bestimmtheit korrespondiert mit dem Grundsatz der Transparenz.

Hier müssen die Erläuterungen über die Datenerhebung „in verständlicher und leicht zugänglicher Form“ sowie „in einer klaren und einfachen Sprache“ verfasst sein.[4] Bei der Art der Erläuterung ist auf den Empfängerhorizont des betroffenen Personenkreises abzustellen.[5] Dies bedeutet, dass die sprachlichen Erläuterungen an den Personenkreis des Empfängerkreises anzupassen sind.

Die Personen, die durchschnittlich die Einwilligung erteilen, müssen in der Lage sein, die Reichweite der Einwilligung abzuschätzen.

Für die Formulierung einer Einwilligung sollten Sie sich immer folgende Fragen stellen, welche idealerweise durch den Einwilligungstext abgedeckt sind:

- Wer soll die Daten nutzen dürfen?
- Welche Dritte sollen die Daten bekommen?
- Was für Daten sollen genutzt werden?
- Welcher Zweckerfüllung dienen die Daten?
- Wie lange wird die Nutzung der Daten andauern?

Sofern sich die Antworten auf die oben genannten Fragen aus dem Einwilligungstext ergeben, ist bereits einen Großteil geschafft.

Freiwilligkeit

Ferner muss eine Einwilligung freiwillig erteilt werden (Art. 7 Abs. 4 DSGVO). Was unter der Freiwilligkeit zu verstehen ist, ist im Gesetzestext nicht definiert. In der Literatur wird hierzu insbesondere die Ansicht vertreten, dass eine Freiwilligkeit im Rahmen der Einwilligung gegeben ist, sofern die einwilligende Person in der Lage ist, die Einwilligung selber abzulehnen oder aber zurückzuziehen, ohne Nachteile zu erleiden.[6] Ein Ausdruck dieses Gebotes der Freiwilligkeit ist auch das sogenannte Kopplungsverbot. Dieses besagt, dass die Erbringung

4 Kühling/Buchner/Buchner/Kühling, 2. Aufl. 2018, DS-GVO Art. 7 Rn. 25, 26
5 BeckOK Datenschutzrecht/Stemmer, 26. Ed. 1.5.2018, DS-GVO Art. 7 Rn. 63.
6 BeckOK Datenschutzrecht/Stemmer, 26. Ed. 1.5.2018, DS-GVO Art. 7 Rn. 38.

einer Leistung nicht an die Erteilung der Einwilligung zur Verwendung personenbezogener Daten geknüpft werden darf.[7] Hier muss allerdings eine klare Abgrenzung vorgenommen werden. Der Gesetzgeber hatte hier z. B. Dienstleistungen vor Augen, bei denen der Verwendung der personenbezogenen Daten zugestimmt werden muss, damit man in den Genuss der Leistung kommt (z. B. Teilnahme an einem Gewinnspiel unter Einwilligung zur Verwendung der personenbezogenen Daten für Werbezwecke). Hiervon abzugrenzen sind Leistungen, bei denen rein faktisch die Verwendung der personenbezogenen Daten für die Erbringung der Leistung selber erforderlich ist. In solchen Fällen muss es weiterhin möglich sein, die Leistung an die Einwilligung zur Verwendung der personenbezogenen Daten zu knüpfen.

Widerrufsmöglichkeit

Der Art. 7 Abs. 3 DSGVO konstituiert die Möglichkeit, jederzeit eine einmal erteilte Einwilligung zu widerrufen. Damit dieses Recht auch wirksam ausgeübt werden kann, muss die Person, welche die Einwilligung erteilt hat, auch über ihr Recht auf einen zukünftigen Widerruf informiert werden.

Diese Information sollte in einem Fließtext immer hervorgehoben und mit den Kontaktdaten für den Widerruf versehen sein. Im Rahmen des Widerrufes gilt ferner noch die Regelung des Art. 7 Abs. 3 S. 4 DSGVO. Nach dieser Vorschrift muss es möglich sein, seinen Widerruf genauso einfach vorzunehmen, wie die ursprüngliche Einwilligung erteilt wurde. Praktisch bedeutet dies, dass keine „künstlichen Hürden“ für den Widerruf aufgebaut werden dürfen. Eine solche Hürde wäre z. B. anzunehmen, wenn eine ursprünglich per E-Mail erteilte Einwilligung später nur per Brief widerrufen werden könnte.

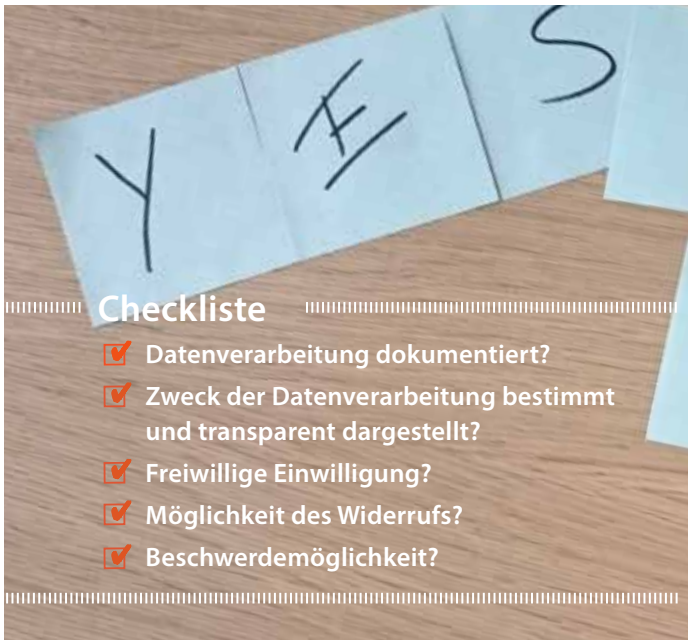
Generell sollten Sie den Weg wählen, dass eine Einwilligung möglichst einfach, d. h. in der Regel auf dem gleichen Weg wie die Einwilligung erteilt wurde, widerrufen werden kann. So stellen Sie immer sicher, dass Ihnen niemand einen Verstoß gegen Art 7 Abs. 3 S. 4 DSGVO zur Last legen kann.

Informationspflichten

Auch wenn ein Großteil der entsprechenden Informationen bereits in einer Einwilligung erläutert werden kann, vergessen Sie nicht, dass es sich bei einer Einwilligung in der Regel um eine neue Erhebung von personenbezogenen Daten handelt. Hier muss grundsätzlich vor Beginn der Datenerhebung gewährleistet sein, dass der betroffenen Person die Informationen nach Art. 13 und Art. 14 DSGVO (Informationspflichten) zur Verfügung gestellt werden.[8]

7 BeckOK Datenschutzrecht/Stemmer DS-GVO Art. 7 Rn. 40.

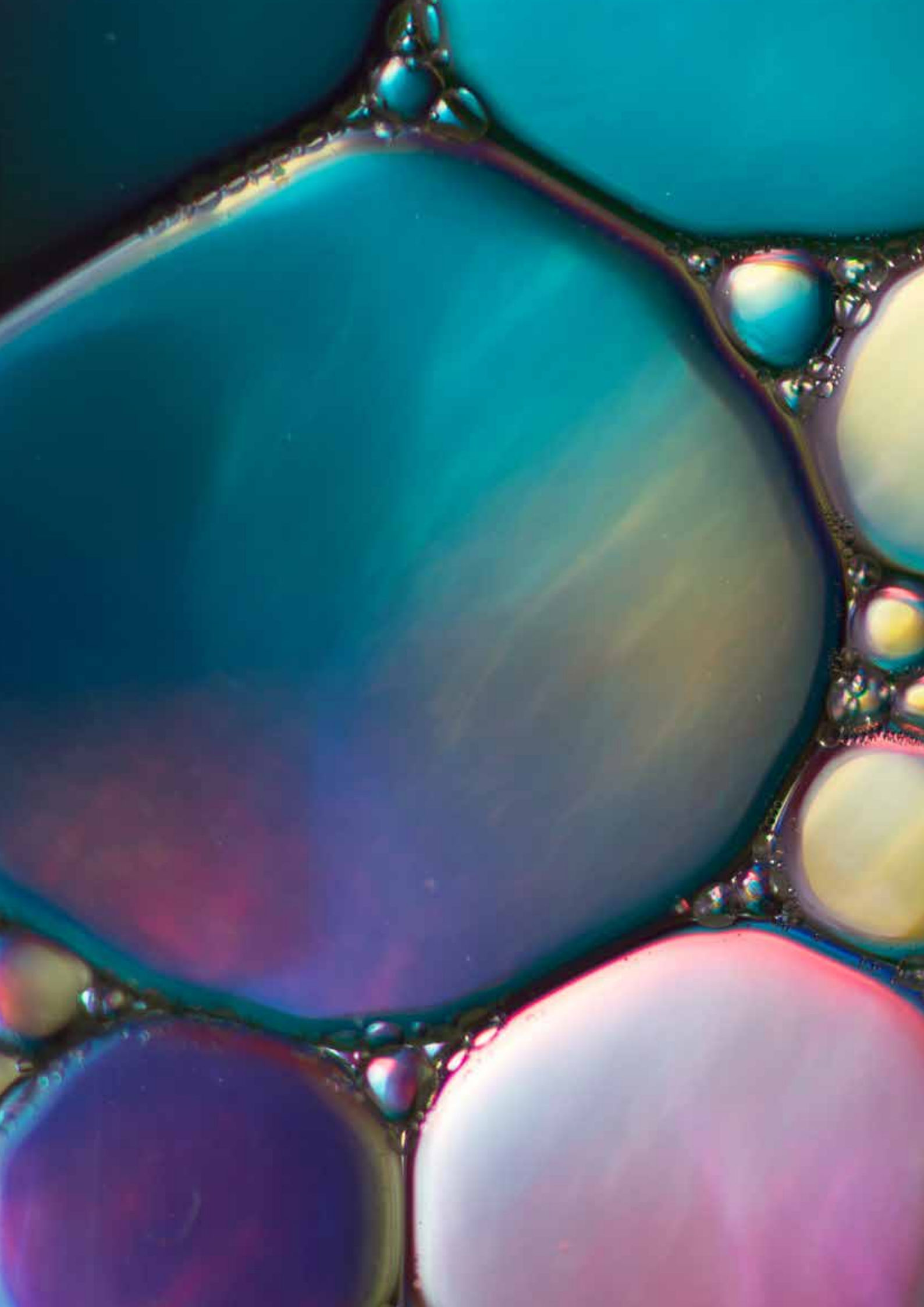
8 Kühling/Buchner/Buchner/Kühling, 2. Aufl. 2018, DS-GVO Art. 7 Rn. 59.



Ass. Jur. Hanjo Tewes

Hanjo Tewes ist Datenschutzbeauftragter und -berater bei der DATATREE AG. Nach seinem Jurastudium an der Universität Bielefeld mit mit dem Schwerpunkt der Wirtschaftsrechtsberatung absolvierte er im Anschluss sein Referendariat am Landgericht Dortmund. Bei der DATATREE AG ist er mit der Implementierung des Datenschutz-Managementsystems, u. a. mit der Gestaltung von Einwilligungserklärungen, Verträgen zur Auftragsverarbeitung und Verfahrensverzeichnissen betraut.

THEMA DER JUNIAUSGABE 2019:

Ein Jahr DSGVO – eine Bestandsaufnahme

Was hat sich wirklich verändert? Wir wagen einen Blick in Unternehmen, befragen Experten und entwickeln Szenarien für die Zukunft.