RISIKOBEURTEILUNG ALS TEIL DER VERANTWORTUNGSBEWUSSTEN DIGITALISIERUNG

Philippe Baumann / Cordula Niklaus / Caroline Walser

Geschäftsführer, integratio GmbH, Börsenstrasse 18, 8001 Zürich, Schweiz
philippe.baumann@integratio.com; https://www.integratio.com
Rechtsanwältin, niclaw, Schifflände 5, 8001 Zürich, Schweiz
Dr. iur., Rechtsanwältin und Lehrbeauftragte an der Law School der Universität St. Gallen, Schweiz
Giblenstrasse 3, 8049 Zürich, CH
caroline.walser@vtxmail.ch; http://www.walserlaw.ch; http://www.visuellesrecht.ch

Schlagworte: ***Risikobeurteilung, Transparenz***

Abstract: *Die Beurteilung eines Risikos im Bereich der Datenverarbeitung unterliegt vielen Einflussfaktoren. Eine standardisierte und transparente Risikobeurteilung ist ein wichtiger Teil für eine verantwortungsbewusste Digitalisierung. Mit der Einführung der DSGVO und der zunehmenden Standardisierung in der IT-Sicherheit durch den Cyber Security Act der EU wird eine erste Basis dafür geschaffen. Neben den Einflussfaktoren und deren Auswirkung auf eine Risikobeurteilung sollen am Beispiel der Beschaffung eines digitalen bildgebenden Gerätes (MRT) in einem Krankenhaus und im Bereich Produkteentwicklung eines Unternehmens die Unterschiede und deren Auswirkung auf die Behandlung eines Risikos aufgezeigt werden.*

1. Einleitung

> *„Die Fähigkeit, Gefahren aus der Umwelt zu erkennen und zu vermeiden, ist für fast alle Lebewesen zur Verbesserung ihrer Überlebenschancen nützlich. Die Fähigkeit, Erfahrungen im Umgang mit der Umwelt zu bewahren und daraus zu lernen, erhöht diese Chancen….“[referenzierung]*

Diese Definition zeigt, dass ein Schlüsselelement für das Anwenden des Erlernten die Risikobeurteilung ist und diese immer wieder neu justiert werden muss, da sich die Umwelt um uns herum fortlaufend verändert.

2. Risikobeurteilung

Die Risikobeurteilung ist bei jedem von uns ein fester Bestandteil zur Bewältigung der Aufgaben, die unser Leben an uns stellt. Risiken werden von Person zu Person unterschiedlich wahrgenommen und somit auch deren Beurteilung und Behandlung.

Am folgenden Beispiel, bei dem Sie die Strasse überqueren wollen und die Fussgänger-Ampel gerade auf Orange umstellt oder das grüne Männchen zu blinken anfängt, soll der Prozess einer Risikobeurteilung beleuchtet werden. Welches sind die Parameter, die in diese Risikobeurteilung einfliessen?

Allgemein gültige Faktoren:

- Wie lange wird noch die Orange Phase beibehalten werden?
- Wie breit ist die Strasse, die ich überqueren will?

Fixe Faktoren:

- Ist gerade ein Polizist in der Nähe, der mich beobachten könnte?
- Wie hoch ist die Verkehrsdichte?

- Wie schnell fahren die wartenden Fahrzeuge an, wenn deren Signal auf Grün geschaltet wird?

Weiterer Einflussfaktor Wetter/Tageszeit:

- Ist es schönes Wetter, Nebel oder regnet es?
- Ist es mitten in der Nacht oder am helllichten Tag?

Persönliche Einflussfaktoren:

- Schuhwerk (von Turnschuh bis Pumps)
- Tagesform
- Alter (18 bis 99)
- Bereits gewonnene Erfahrung an diesem Strassenübergang durch frühere Versuche

Situative Einflussfaktoren:

- Habe ich noch genügend Zeit zur Erreichung meines Ziels?

Obwohl es für diese Entscheidung nur zwei Ergebnisse geben kann (Warten oder Gehen) ist schon an diesem Beispiel die Fülle an möglichen Einflussfaktoren sichtbar.

2.1. Persönliches Umfeld

Wie ein Risiko eingeschätzt wird und ob ein Risiko überhaupt als solches wahrgenommen wird hängt massgeblich vom Umfeld, von der Bildung, dem Wissen, Können und der Erfahrung des Betrachters ab.

> *Ein Sprungschanzenteilnehmer wird den Sprung von einer Sprungschanze anders beurteilen als jemand, der noch nie von einer Schanze gesprungen ist.*

2.2. Bedeutung der individuellen Risikowahrnehmung

Die individuelle Risikowahrnehmung ist wichtig. Der Sportliche, der Zu-spät-Kommende, die Rentnerin: Jede Person interpretiert und bewertet die gleiche Situation an der Ampel unterschiedlich und somit wird auch die Risikobeurteilung unterschiedlich ausfallen.

Ob ein Sachverhalt ein Risiko darstellt oder nicht liegt im Auge des Betrachters.

2.3. Nachträgliche Bewertung von Risikobeurteilungen

Die Schaffung einer einheitlichen Wissensbasis (Standards), die für die Erstellung und Bewertung von Risikobeurteilungen herangezogen werden kann, ist ein Muss für eine nachträgliche Bewertung von Risikobeurteilungen.

2.4. Risikobeurteilung bei personenbezogenen Daten

Die Risikobeurteilung der Verarbeitung personenbezogener Daten hat zum Ziel, die Bewertung der Eintrittswahrscheinlichkeit und Schwere von Risiken für die Rechte und Freiheiten natürlicher Personen zu bestimmen. Neben den organisatorischen Massnahmen, die den Umgang mit personenbezogenen Daten definieren, ist die IT-Sicherheit von zentraler Bedeutung.

Hierbei sind folgende Felder zu berücksichtigen:

- Vertraulichkeit: Der Zugriff auf die Daten ist auf die Personen und Systeme einzugrenzen, die für die Verarbeitung der Daten den Zugriff benötigen.
- Integrität: Sicherstellung der Korrektheit von Daten und Verhinderung von unerkannten Veränderungen an den Daten.

- Verfügbarkeit: Sicherstellen, dass die Daten jederzeit zur Verfügung stehen und mögliche Ausfälle der betroffenen Systeme auf ein Minimum zu reduzieren sind.

3. Gesetze, Standards und Richtlinien zu personenbezogenen Daten

3.1. Personenbezogene Daten

Die Etablierung von branchenübergreifenden Standards rund um das Thema *personenbezogene Daten* und deren Umsetzung hat noch keine lange Historie und die Ahndung von Unternehmen bei Fehlverhalten steckt noch in den Kinderschuhen. In einzelnen Branchen (Ärzte- und Anwaltsgeheimnis) und anderen Bereichen (Industrie, Pharma etc.) sind die Regulatorien schon viel weiter entwickelt.

3.2. Europäische Datenschutz Grundverordnung (DSGVO)

Die DSGVO regelt den Umgang mit personenbezogenen Daten und deren Schutz und schafft damit europaweit (EU/EWR) ein einheitliches Grundverständnis und Regelwerke für den Umgang mit personenbezogenen Daten, flankiert von wirksamer Sanktionierung bei Fehlverhalten.

Die Diskussionen, die heute rund um die DSGVO geführt werden, erinnern stark an die Diskussionen bei der Einführung des Sicherheitsgurtes im Auto. Damals wurde die Sinnhaftigkeit dieser Vorschrift sehr kontrovers diskutiert und heute ist die Tragepflicht von Sicherheitsgurten kein Diskussionsthema mehr, sondern eine Selbstverständlichkeit.

3.3. Akzeptanz in anderen Bereichen

Während im Bereich des Datenschutzes und der Personlichkeitsrechte, deren Schutz eine Basis für eine verantwortungsvolle Digitalisierung ist, Standards und Regulatorien noch mit Skepsis und Ablehnung betrachtet werden, ist die Nutzung von Motorfahrzeugen heute ohne die Anwendung von Standards und Regulatorien undenkbar. Der Crashtest für Fahrzeuge oder der Test zur Messung des Treibstoff-Verbrauchs dürften für die Meisten ein Begriff sein und dienen in der Regel als Parameter für die Entscheidungshilfe bei der Beschaffung von Fahrzeugen. Der Einsatz von Standards bei der Entwicklung, Produktion und Betrieb von Motorfahrzeugen wird nicht mehr in Frage gestellt. Das schlechte Abschneiden in Tests hat Auswirkungen auf die Verkaufszahlen oder kann auch zu Rückrufaktionen führen.

4. Gesetze, Standards und Richtlinien zur IT-Sicherheit

4.1. IT-Sicherheit im Allgemeinen

Die IT-Sicherheit, früher ausschliesslich ein Thema von IT-Sicherheitsspezialisten, tritt durch die verschiedenen medienwirksamen Cyber-Angriffe in Unternehmen immer mehr ins Zentrum der Gesellschaft. Die Informationstechnologie durchdringt immer schneller alle Bereiche unseres Lebens und dadurch wird IT-Sicherheit immer mehr ein Thema, mit dem sich jede Person auseinandersetzen sollte. Das Niveau der IT-Sicherheit definiert heute massgeblich die Integrität, Souveränität und Unabhängigkeit einer einzelnen Person, eines Unternehmens, einer Gesellschaft oder eines Staates.

4.2. IKT-Minimalstandards des Bundes (CH)

Mit dem IKT-Minimalstandard des Bundes wird mittels eines Fragenkatalogs auf einem sehr groben Level der Status bei Unternehmen abgefragt. Implizit werden dadurch Empfehlungen für einen Minimalstandard im Bereich IT-Sicherheit gesetzt ohne auf die konkrete Umsetzung dieser einzugehen. Ein (kleiner) Schritt in die richtige Richtung.

4.3. ISO 27001

Die ISO 27001 ist ein Standard zur Etablierung eines *Information Security Management Systems* (ISMS) in Unternehmen. Ein ISMS ist ein systematischer Ansatz zur Verwaltung vertraulicher Unternehmensinformationen, damit diese sicher bleiben. Es umfasst Personen, Prozesse und IT-Systeme, indem ein Risikomanagementprozess angewendet wird. Mit der ISO 27001 werden auch regelmässige Überprüfungen zur Sicherstellung der Aktualität der umgesetzten IT-Sicherheitsmassnahmen implementiert.

4.4. BSI IT-Grundschutz

Der IT-Grundschutz ist ein vom BSI (Deutschland) entwickeltes systematisches Vorgehen, notwendige Sicherheitsmaßnahmen für Institutionen zu identifizieren und umzusetzen. Er dient dazu, „das Niveau der Informationssicherheit in Behörden und Unternehmen jeder Größenordnung zu erhöhen“. Der BSI IT-Grundschutz stellt nicht nur einen Fragenkatalog zur Verfügung sondern bietet und fordert Lösungen zur Behebung oder Minimierung von Risiken. Der BSI IT-Grundschutz definiert drei Sicherheitsstufen und gibt auch gleich vor welche Stufe für welches Unternehmen mit welchen Anforderungen anzuwenden wäre.

4.5. Cyber Security Act der EU

Der Cyber Security Act der EU ist die Antwort auf die Gefahrenlage mit dem Ziel EU-übergreifend einen einheitlichen Massnahmenkatalog zu definieren und eine EU-übergreifende Behörde (ENSIA) zu schaffen zur Förderung des Problembewusstseins im Bereich der Cybersicherheit und der Unterstützung zur Schaffung politischer Rahmenbedingungen.

Das Augenmerk des Cyber Security Act der EU liegt gegenwärtig auf der Sicherstellung der Funktionstauglichkeit der kritischen Infrastrukturen (KRITIS) in Europa (Wasser- und Stromversorgung, Banken- und Versicherungsinfrastruktur etc.). ENSIA wird Cybersicherheitszertifizierung für spezifische IKT-Prozesse, Produkte und Dienste schaffen. Im Rahmen dieser Systeme ausgestellte Zertifikate werden in allen EU-Ländern gültig sein, wodurch das Vertrauen der Nutzer in die Sicherheit dieser Technologien gestärkt und es den Unternehmen leichter gemacht wird, ihre Geschäftstätigkeit über Ländergrenzen hinweg auszuüben.

4.6. Einordnung der Standards

Gemessen am BSI IT-Grundschutz orientiert sich der IKT-Minimalstandard des Bundes an der Stufe 1 des IT-Grundschutzes. Die ISO 27001 ist mit dem BSI IT-Grundschutz ab Stufe 2 vergleichbar. Die Stufe drei des BSI IT-Grundschutzes zielt auf die Abdeckung IT-sicherheitsrelevanter Massnahmen für kritische Infrastrukturen (KRITIS). Der IT-Grundschutz liefert gegenüber ISO 27001 konkrete Handlungsempfehlungen, die eine Umsetzung erleichtern. Die Anwendung der hier angewandten Standards bei der Entwicklung von IKT-Produkten wird die Basis für die Erlangung der ENISA-Zertifikate sein. Die ENISA wird die Zusammenarbeit der EU-Mitgliedstaaten im Bereich Cybersecurity fördern und mit der Einführung von Zertifikaten für IKT-Produkte, welche in allen EU-Mitgliedstaaten Gültigkeit haben, den Zugang zu den verschiedenen Märkten für anerkannt sichere IKT-Produkte vereinheitlichen und erleichtern.

5. Risikobeurteilungen anhand von Beispielen

5.1. Beispiel Insulinpumpe

5.1.1. Kurzbeschreibung

Mit einer mobilen Insulinpumpe wird dem Patienten, entsprechend der durch den Arzt vorgenommenen Einstellung, regelmässig Insulin verabreicht. In der Regel hat der Patient zusätzlich die Möglichkeit, sich bei Bedarf manuell eine Dosis Insulin zu verabreichen. Die Verabreichungen werden geloggt und in regelmässi-

gen Abständen durch den Arzt ausgewertet. Auf Grund der Auswertung wird die Einstellung der Insulinpumpe kontrolliert und wo notwendig nachjustiert.

5.1.2. Risikobeurteilung bei der Entwicklung und Nutzung einer Insulinpumpe

Die Entwicklung von Insulinpumpen erfordert eine hohe Investition in Tests. Risikobeurteilungen der Hardware gehören hier schon lange zum Tagesgeschäft und werden auch durch Regulatorien (MDD/MDR) eingefordert. Auf dieser Basis konnte in einem konkreten Praxisfall die Implementierung zusätzlicher Risikobeurteilungen im Bereich Datenschutz und personenbezogene Daten (hier bei den Log-Daten) mit wenig Aufwand sachgerecht und zielgerichtet erfolgen.

Rund um die zu verarbeitenden Daten wurden folgende Fragen geklärt:

- Welche Daten werden erhoben? Welche Daten sollen nicht erhoben werden?
- Wer hat Zugang zu den erhobenen Daten?
- Werden Daten an Dritte weitergegeben?
- In welchem Detaillierungsgrad werden Daten weitergegeben?
- Sind die einzelnen Übergänge des Datenflusses technisch wie rechtlich geregelt?

5.1.3. Ausweitung der Risikobeurteilung im Bereich Anwendungstest

In diesem Fall wurden nicht nur die zu verarbeitenden Daten der Insulinpumpe einer Risikobeurteilung unterzogen, sondern auch die Durchführung der Anwendungstest bei der Erprobung durch Probanden. Dabei ist bei der Weitergabe der Ergebnisse die Anonymität der Probanden sicherzustellen. Beispielsweise wurden bei den Anwendungstests Video-Aufnahmen vorgenommen und es muss sichergestellt werden, dass die Probanden auf den Aufzeichnungen nicht erkennbar sind.

5.2. Beispiel die Beschaffung eines MagnetResonanzTomographen (MRT)

5.2.1. Kurzbeschreibung

Die Magnetresonanz-Tomographie ist ein bildgebendes Verfahren zur Darstellung von Strukturen im Inneren des Körpers. Sie kann Schnittbilder des menschlichen Körpers in beliebigen Ebenen erzeugen. Aus den Daten können per Computer 3D-Datensätze berechnet werden.[MRT]

5.2.2. Installation und Betrieb eines MRT

Der Betrieb eines MRTs ist extrem kostenintensiv. Für eine effektive Amortisation der Anschaffung eines MRT sind die Ausfallzeiten möglichst gering zu halten. Die Wartung eines MRTs wird in der Regel an den Hersteller delegiert. Die Vor-Ort-Wartung des MRT wird stark durch die Möglichkeit der Fernwartung für eine Gerätediagnose oder Behebung von Störungen durch Fehlbedienungen ergänzt. Für die Fernwartung muss IT-technisch ein Zugang gelegt werden, damit der Zugriff auf das MRT von Aussen möglich ist. Dieser Zugang macht die IT-Infrastruktur eines Krankenhauses verletzlich und muss durch geeignete Massnahmen abgesichert werden, bzw. komplexe Geräte wie das MRT müssen wiederum von der restlichen IT-Infrastruktur des Krankenhauses gesondert behandelt und abgesichert werden.

5.2.3. Risikobeurteilung zu einem MRT

Bei einer Risikobeurteilung zum Einsatz eines MRT ist es nicht mehr ausreichend, das MRT und die durch das MRT erzeugten Daten in die Betrachtung einzubeziehen. Die Sicht verlagert sich mehr auf das Umfeld des MRT - das gesamte Krankenhaus - dessen Integrität und Verfügbarkeit auch bei einem Einsatz komplexer Gerät wie einem MRT sichergestellt werden muss. In einem konkreten Fall einer Sicherheitsüberprüfung waren viele Ports geöffnet, um den Zugang zum MRT zu gewährleisten – und damit war die Sicherheit des

gesamten Krankenhauses gefährdet. Die Bewertung des Herstellers eines MRT zum Thema Wartung und Betrieb wird eine sehr hohe Gewichtung in einer Risikobeurteilung bekommen.

5.3. Umsetzung von Risikobeurteilungen

5.3.1. Hersteller – alles was möglich ist

In einigen Branchen wie beispielsweise der Medizintechnik ist die Entwicklung und Herstellung von Produkten heute schon stark reglementiert. Medizinische Produkte benötigen eine Marktfreigabe, die wiederum nur dann vergeben wird, wenn die erforderlichen Dokumentationen und Studien eine Unbedenklichkeit attestieren. Die Erweiterung der Prozesse um die Dimension personenbezogene Daten ist hier als ein eher kleiner Aufwand anzusehen.

Bei der Entwicklung von digitalen Produkten und Software und der einhergehenden Datensammlung und –verarbeitung gibt es häufig keine vorgängige Risikobeurteilung. Man entwickelt was möglich ist. Mit der Einführung und Umsetzung der DSGVO und der damit verbundenen Einführung von Risikobeurteilungen von Datenverarbeitungen bereits während der Software-Entwicklung tun sich die Unternehmen heute immer noch schwer.

5.3.2. Anwender – Haben wollen

Die Evaluation neuer Produkte und neuer Dienstleistungen ist oftmals durch das „haben wollen“ angetrieben. Die Präferenz für ein spezifisches Produkt oder eine spezifische Dienstleistung beeinflusst die Entscheidungsfindung und nimmt Einfluss auf die Wahrnehmung von Risiken. Eine Risikoeinstufung basierend auf Standards ist hier kein Allheilmittel, hilft jedoch die Entscheidung basierend auf der Gewichtung der Risiken zu verstehen und macht die Entscheidung zumindest im Risikobereich überprüfbar.

Bei der Insulinpumpe haben mögliche Risiken durch Datenverlust der gewonnen Daten für die Patienten eine untergeordnete Rolle, da bei diesem Produkt der Mehrwert an Lebensqualität und gewonnene Flexibilität gegenüber früheren Lösungen mögliche Bedenken bei weitem überwiegen wird.

Der Entscheid für ein bestimmtes MRT auf Grund umfangreicherer Features, welches möglicherweise einen tiefen Sicherheitslevel nach sich zieht muss sichtbar gemacht werden, damit in der IT-Abteilung des Krankenhauses entsprechende Massnahmen getroffen werden können um diese Schwachstellen zu eliminieren.

5.4. Risiken in den Griff bekommen

Risiken lassen sich in den Griff bekommen. Dies ist jedoch nur möglich, wenn diese analysiert, bewertet, dokumentiert und visualisiert werden.

Am Beispiel der Insulinpumpe zeigte sich, dass es sich hier um überschaubare und eingegrenzte Prozesse handelt und der Fluss der Daten bis hin zu möglichen Studien durch den auftraggebenden Pharmakonzern nachvollziehbar und vertraglich geregelt ist.

Am Beispiel des MRT zeigte sich, dass das frühe Einbeziehen der IT-Abteilung in die Evaluation eines MRT notwendig ist, damit die IT-Abteilung rechtzeitig Massnahmen zur Sicherung des Betriebes des Krankenhauses erarbeiten kann.

6. Schlussfolgerung

Die Anwendung und Dokumentation von Risikobeurteilungen der Verarbeitung und Speicherung von personenbezogenen Daten ist eine logische Fortsetzung von Risikobeurteilungen aus Industrie und Produkteentwicklung. Je mehr Standards und Regulatorien zur Risikominimierung in einer Branche bereits vorhanden sind und angewandt werden, desto kleiner ist der Schritt zur Risikobeurteilung der Verarbeitung personenbezogener Daten. Branchen, die bisher nicht reguliert sind, tun sich noch schwerer.

6.1. Umfang

Eine Risikobeurteilung ist nur möglich, wenn alle betroffenen Bereiche in und ausserhalb des Unternehmens einbezogen werden. In einem Unternehmen ist daher oftmals nur auf Ebene der Geschäftsleitung erkennbar, welche Daten wo zu welchem Zweck verarbeitet werden, unter der Voraussetzung natürlich, dass diese dokumentiert sind. Durch die Einführung der DSGVO ist die Geschäftsleitung eines Unternehmens in der Pflicht, Massnahmen zur Einhaltung der Gesetze bei der Bearbeitung von personenbezogenen Daten einzuführen, umzusetzen und zu kontrollieren.

6.2. Überprüfbarkeit

Die Risikobeurteilung als Teil der Dokumentation zur Verarbeitung und Speicherung von personenbezogenen Daten dient als Nachweis, dass sich ein Unternehmen bereits frühzeitig über die Risiken Gedanken gemacht hat. Damit die Einhaltung von Vorschriften und Standards überprüft werden kann, müssen die getroffenen Massnahmen in den Unternehmen dokumentiert und kontrollierbar gemacht werden. Die Überprüfbarkeit von Risikobeurteilungen lässt sich effizient nur auf Basis von Standards und Vorgaben umsetzen. Die Grundlage einer Risikobeurteilung zu dokumentieren erfordert Übung und in der „Eingewöhungszeit“ einen Mehraufwand.

6.3. Ahndung

Es hat sich gezeigt, dass Vorschriften nur zögerlich umgesetzt werden, wenn bei Nichteinhaltung keine Strafen zu befürchten sind. Die Ahndung bei Nichteinhaltung von Vorschriften ist notwendig und gegenüber denjenigen Unternehmen, die sich an die vorgegebenen Regelwerke halten, Pflicht im Sinne einer verantwortungsbewussten Digitalisierung.

Mit einer standardisierten Risikobeurteilung kann jedes Unternehmen für sich abwägen, wie ihre Produkte und Dienstleistungen zu gestalten sind und rechtzeitig Massnahmen und Anpassungen vornehmen, um solche Bestrafungen zu verhindern.

6.4. Initialer Mehraufwand

Die Implementierung einer Risikobeurteilung erzeugt in Unternehmen, die bis anhin noch keine Risikobeurteilungen implementiert haben, initial einen erheblichen Aufwand. Dies umfasst die Sensibilisierung und Schärfung der Wahrnehmung der Mitarbeiter für das Thema Risiko, die Einführung von Methodiken und die Schulung der Mitarbeiter für die Durchführung von Risikobeurteilungen.

6.5. Änderungen in den Prozessen

Die Implementierung von Risikobeurteilungen erfordert Anpassungen in bestehenden Prozessen. Bei der Entwicklung von Software-Lösungen können Risikobeurteilungen zum frühen Zeitpunkt der Konzeptionierung mögliche Fehlentwicklungen verhindern. Dies zieht allerdings Änderungen in der Software-Entwicklungsprozessen nach sich. Beispielweise müssen in agile Methoden regulatorischen Anforderungen und Risikobetrachtungen einbezogen werden.

6.6. Mehrwert

Die Vorteile einer Risikobeurteilung generell und im speziellen bei personenbezogenen Daten liegen auf der Hand:

- erhöhter Dokumentationsgrad
- fundierte Entscheidungsgrundlage
- verbessertes Risikomanagement und damit Risikosenkung
- Compliance

6.7. Nachvollziehbarkeit und Transparenz

Entscheidungen können auch in Zukunft auf Basis einer zugrundeliegenden und standardisierten Dokumentation von Risikobeurteilungen (besser) nachvollzogen werden.

Das Risiko eines digitalen Produktes könnte dem Betroffenen gegenüber transparent gemacht und visualisiert werden (z.B. mit einem Ampelsystem). Den Betroffenen in die Lage zu versetzen, sein Risiko auf einfache Weise basierend auf Standards zu beurteilen, ist Teil einer verantwortungsvollen Digitalisierung.

6.8. Risikobeurteilung als wiederkehrende Aufgabe

Es ist nicht absehbar, welche Auswertungen in der Zukunft mit den gewonnen Daten von heute vorgenommen werden können. Aus diesem Grund ist es notwendig die Risikobeurteilung von Verarbeitungen und Speicherungen von personenbezogenen Daten als wiederkehrende Aufgabe zu implementieren, die sich an neuen und angepassten Standards orientieren.

Denn: Was heute mit personenbezogenen Daten erlaubt ist, ist morgen vielleicht verboten.

6.9. Reputationsschutz

Durch die Verletzung von datenschutzrechtlichen Vorschriften kann die Reputation eines Unternehmens Schaden nehmen. In diesem Sinne sind aktuell geführte Risikobeurteilungen zur Verarbeitung personenbezogener Daten im Interesse eines jeden Unternehmens.

7. Ausblick

Welche Daten gesammelt und wie diese in Zukunft verwendet und verknüpft werden können lässt sich heute nur erahnen. Die Verfeinerung der Aufzeichnungen von personenbezogenen Daten und deren Verarbeitung und Auswertung wird uns in allen privaten Bereiche durchdringen.

Aus diesem Grund sind Vorschriften, Standards und Regelwerke notwendig, damit Risiken gemessen, verglichen, kommuniziert und visualisiert werden können und eine verantwortungsbewusste Digitalisierung nicht zu einer Illusion wird.

8. Literatur

Chauncey Starr/Adalbert Evers/ Niklas Luhmann/Ulrich Beck/Helga Nowotny/Gotthard Bechmann/Karl-Heinz Ladeur/Mario Cogoy/Klaus-Dieter Nowitzki/Klaus P. Japp/Stanley Kaplan/Jon Elster/Roland Kollert/B. John Garrick, Die Psychologie der Kognition und Evaluation von Risiko, Westdeutscher Verlag GmbH, Opladen, 1993.

Rossella Mattioli/Dr. Cédric Levy-Bencheton , Methodologies for the identification of Critical Information Infrastructure assets and services - Guidelines for charting electronic data communication networks, European Union Agency for Network and Information Security (ENISA) , Heraklion, 2014.

Dr. med. Christoph Pabst, Grundlagen der Magnetresonanz-Tomographie, UKGM Standort Marburg, 2013

Dietmar Bestenlehner/Gerald Boyne/Bertram Dorn/Günter Eggers/Markus Feichtner/Dr. Joachim Fölsch/Hans-Jürgen Gerhards/Gerd Giese Akamai/Michael Kranawetter Microsoft/Lars Nadzeyka/Dr. Dietmar Otten/Sunita Ute Saxena/Dr. Pascal Schmidt/Volker Rauscher/René Wienholtz, 2018, Branchenspezifischer Sicherheitsstandard zur IT-Sicherheit - UP KRITIS - BAK Datacenter & Hosting mit CDN, 2018-04-30_B3S_BAK_DCH_V1.05.

Prof. Dr. Helmut Jungermann, Zur Wahrnehmung und Akzeptierung des Risikos von Großtechnologien, in Psychologische Rundschau, 33, 1982, S. 217-238.

Mössner Thomas, Risikobeurteilung im Maschinenbau, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, 2012.

Kritische Infrastrukturen - Definition und Übersicht, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe & Bundesamt für Sicherheit in der Informationstechnik, https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.htm.

Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, D, AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, 2018.

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

DIN EN ISO/IEC 27001:2017-06, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen Fassung EN ISO/IEC 27001:2017, Beuth publishing DIN, 2017 [referenz auf literatur bsi]

Medical Device Regulation MDR – Medizinprodukteverordnung (2017/745), EU-Parlament, 5.4.2017