Ausgabe 1 Februar 2018

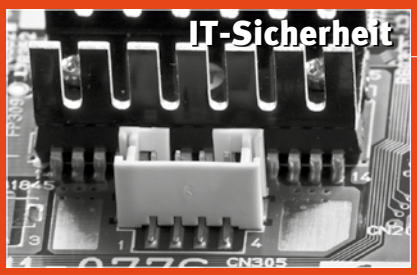
Revisionspraxis

PRev

Journal für Data Science, IT-Sicherheit, SAP-Sicherheit und Datenschutz

Rainer Feldmann
Statistisches Denken für Prüfer (Teil 7) – Lineare Regression (1)

Erwin Rödler
Eine Übersicht risikoorientierter Ansätze im Bereich Data Science



Marc Alexander Luge
Modernisierung des IT-Grundschutzes und der Leitfaden zur Basis-Absicherung nach IT-Grundschutz

Ingo Köhne
Blockchain – DIE Zukunftstechnologie?!

Kai Henken
KRACK: Eine Angriffsmöglichkeit auf die WPA2 WLAN-Verschlüsselung

Christoph Wildensee
Prüfung der SAP-Berechtigungen in der Digitalen Personalakte von XFT

Antonio Ralf W. Reschke/Maximilian Schmidt
IT-Sicherheit gemäß der EU-DSGVO! Wonach haben sich Unternehmen zu richten?

Check-Up Datenschutz

Rechtsprechung und Aktuelles zum Datenschutz

www.prev.de

ISSN 1862-9032

BOORBERG

Antonio Ralf W. Reschke

Maximilian Schmidt

Datenschutz

IT-Sicherheit gemäß der EU-DSGVO! Wonach haben sich Unternehmen zu richten?

Ist die IT-Sicherheit überhaupt Bestandteil der Europäischen Datenschutz-Grundverordnung oder ist sie nicht anderweitig geregelt?

IT-Sicherheit ist ein Querschnittsthema, das viele andere Themengefüge beeinflusst. Sie muss immer im Kontext der Schutzgegenstände gesehen und für das jeweilige Einsatzgebiet angepasst werden.[1] So bestehen mit dem Datenschutz einige „Schnittmengen", schließlich ist die Wahrung des verfassungsrechtlich garantierten allgemeinen Persönlichkeitsrechts ohne einen wirksamen Schutz der personenbezogenen Daten (im Folgenden Daten) nicht effektiv möglich.

Der Begriff „IT-Sicherheit" oder „Informationssicherheit" wird überwiegend mit den klassischen Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität in Verbindung gebracht.[2] Insoweit ist eine Überschneidung mit dem Datenschutz anerkannt. Im Kontext des Datenschutzes kann der Begriff jedoch weiter gefasst werden. Darunter sind schließlich alle „technischen und organisatorischen Maßnahmen" zu verstehen, die den Schutz der Daten und des allgemeinen Persönlichkeitsrechts sicherstellen können. Die einzelnen Maßnahmen lassen sich dabei nicht immer nur einem der beiden Bereiche zuordnen.

1 Tinnefeld/Bucher/Petri, S. 415.

2 Vgl. Gola/Schomerus/*Körffer/Gola/Klug*, § 9 BDSG, Rn. 1–6.

Aus den zuvor genannten Gründen liegt der Fokus der vorliegenden Betrachtung nicht ausschließlich auf dem „klassischen Bereich" der IT-Sicherheit. Vielmehr werden die Regelungen der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) über technische und organisatorische Maßnahmen zur Umsetzung des Datenschutzes in die Betrachtung mit einbezogen.

Aufgrund der negativen Erfahrungen mit § 9a Bundesdatenschutzgesetz (BDSG – alt) und damit im direkten Zusammenhang stehender Institutionen wird bewusst nicht auf Verhaltensregeln und genehmigte Zertifizierungsverfahren – im Rahmen der zuvor genannten Vorschrift – eingegangen.

Wie sehen die rechtlichen Rahmenbedingungen derzeit aus? Basiert das Bundesdatenschutzgesetz (alt) auf veralteten Rahmenvorgaben?

Grundsatz der (altbewährten) Verhältnismäßigkeit!

Schon das inzwischen annähernd vierzig Jahre alte BDSG (alt) regelte in der ersten Fassung, dass technische und organisatorische Maßnahmen zu treffen sind, um die Anforderungen des Gesetzes zu erfüllen. Die Anforderungen sind auch in der aktuellen Fassung – im Kern unverändert – enthalten. Die Maßnahmen stellen demnach keinen Selbstzweck dar, vielmehr sind sie deshalb anzuwenden, um die Gebots- und Verbotsnormen in technischer sowie organisatorischer Hinsicht flankierend zu unterstützen. Dies bedeutet jedoch nicht, dass die verantwortliche Stelle in jedem Fall eine Wahlmöglichkeit hinsichtlich des „Ob" einer Maßnahme hat, da Maßnahmen grundsätzlich konstitutiv für die Rechtmäßigkeit des Betreibens von Verfahren sind.

§ 9 BDSG (alt) sieht vor, dass technische und organisatorische Maßnahmen getroffen werden müssen, um die Ausführung der Vorschriften des BDSG (alt) zu gewährleisten. Die technischen und organisatorischen Maßnahmen müssen sich dabei immer am Zweck des BDSG (alt), nämlich dem Schutz vor Beeinträchtigung des allgemeinen Persönlichkeitsrechts, ausrichten. Das Gesetz sieht dabei nicht nur Maßnahmen vor, um die klassischen Ziele der IT-Sicherheit zu gewährleisten, sondern spricht den technischen und organisatorischen Maßnahmen auch die Aufgabe zu, grundsätzlich alle datenschutzrechtlichen Vorgaben – nicht lediglich die Schnittmenge mit der IT-Sicherheit – umzusetzen.[3]

Allerdings sind gemäß Satz 2 nur solche Maßnahmen zu treffen, die im Rahmen einer Verhältnismäßigkeitsprüfung als erforderlich erachtet werden.[4] Dies ist dann der Fall, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Mit der Orientierung am Schutzzweck wird deutlich, dass der Schutz der personenbezogenen Daten des Betroffenen und mithin seine Selbstbestimmung im Vordergrund stehen. Der vom Gesetzgeber gewählte Begriff „Schutzzweck" ist jedoch irreführend. Vielmehr dürfte in diesem Zusammenhang der Begriff „Schutzbedürftigkeit" der Daten des Betroffenen zutreffender sein, schließlich werden sich die Maßnahmen im konkreten Einzelfall daran ausrichten. Die Schutzbedürftigkeit ergibt sich aus der Art der Daten, dem Zweck und Umfang und dem Schadenspotenzial bei Verlust oder unzulässiger Verarbeitung.[5]

Eine Einstufung der Verarbeitungen oder Daten nach Schutzstufen ist daher zweckmäßig. Den definierten Schutzstufen können generische Sicherheitsmaßnahmen zugeordnet werden, sodass sich aus der Klassifizierung der Daten unmittelbar die erforderlichen Maßnahmen ableiten lassen. Dabei bilden im Falle der Verwendung unterschiedlicher Datenarten stets die sensibelsten Daten den Maßstab für die Schutzbedürftigkeit.[6]

Anforderungskatalog nicht mehr praxiskonform?

Bei der Anlage zu § 9 BDSG (alt) handelt es sich um einen Kompromiss zwischen einerseits einer allgemeinen sowie flexiblen Formulierung und andererseits dem Praxisbedürfnis nach konkreten Maßnahmenvorgaben.[7] Die Anlage enthält eine Auflistung von Zielvorgaben, die die Einhaltung der Datenschutzregelungen sicherstellen helfen sollen. Es wird differenziert zwischen neun (die Organisationskontrolle eingerechnet) verschiedenen Kontrollformen, wobei sich die erforderlichen Maßnahmen zumeist mehreren Kontrollaufgaben zuordnen lassen. Welche Maßnahmen im Einzelnen umgesetzt werden, richtet sich nach den besonderen Umständen sowie Gegebenheiten im konkreten Anwendungsfall und kann von den datenverarbeitenden Stellen selbst gewählt werden.

Die Kontrollen bilden das Mindestmaß an Sicherheitsmaßnahmen, die die verarbeitende Stelle zur Gewährleistung des BDSG (alt) zu ergreifen hat.

3 Vgl. Simitis, § 9 BDSG Rn. 47–56.
4 Plath/*Plath*, § 9 BDSG Rn. 3.
5 Plath/*Plath*, § 9 BDSG Rn. 16.
6 Plath/*Plath*, § 9 BDSG Rn. 17.
7 Plath/*Plath*, § 9 BDSG Rn. 21.

Umsetzung in der Praxis! Geht das überhaupt noch?

Da weder § 9 BDSG (alt) noch das BDSG in seiner Gesamtheit einen konkreten Verweis auf eine risikobasierte Bewertung der datenverarbeitenden Prozesse bzw. Verarbeitungsverfahren enthält, erfolgt in der praktischen Umsetzung des § 9 BDSG (alt) und seiner Anlage eine solche in der Regel auch nicht. Vielmehr ist in der Praxis festzustellen, dass der Katalog aus der Anlage zu § 9 BDSG (alt) dazu herangezogen wird, die eigenen, getroffenen Maßnahmen zu dokumentieren und auch für Dritte darzustellen. Den einzelnen Kontrollzielen werden dabei – aus Sicht eines Dritten – scheinbar „willkürlich" Maßnahmen zugeordnet.

Diese Maßnahmenbeschreibungen können sehr abstrakter Natur sein und beziehen sich oftmals auf das gesamte Unternehmen. Einzelne Verfahren oder Prozesse werden nicht berücksichtigt. In dieser Vorgehensweise besteht für Unternehmen das Risiko, dass interessierten und berechtigten Dritten, beispielsweise der Datenschutz-Aufsichtsbehörde, nicht glaubhaft gemacht werden kann, dass geeignete Maßnahmen getroffen wurden.

Es ist aber dennoch davon auszugehen, dass in der betrieblichen Praxis die verschiedenen Ausprägungsformen des Anforderungskatalogs auch nach Inkrafttreten der EU-DSGVO noch einige Zeit erhalten bleiben.

Brauchbare Regelungen der EU-DSGVO für die IT-Sicherheit! Oder wird es (noch) schlechter?

Technische und organisatorische Maßnahmen sind grundsätzlich „tot"!

Eine einzige Norm, aus der alle Anforderungen zu den technischen und organisatorischen Maßnahmen hervorgehen – so wie im BDSG (alt) mit § 9 und dessen Anlage – existiert in der EU-DSGVO nicht. Vielmehr verteilen sich die Anforderungen an die Maßnahmen auf drei Artikel mit mehr oder weniger konkreten Vorgaben. Darüber hinaus hat neben den Artikeln 24, 25 und 32 EU-DSGVO auch Artikel 35 EU-DSGVO (Datenschutz-Folgenabschätzung) Einfluss auf die Ausgestaltung der Datenschutzmaßnahmen.

Artikel 24 EU-DSGVO als allgemeine Risikobewertungsgrundlage?

Der Normensystematik nach liegt mit Artikel 24 EU-DSGVO eine Generalnorm zu den technischen und organisatorischen Maßnahmen nach der EU-DSGVO vor. Darin wird vom Verantwortlichen die Umsetzung geeigneter technischer und organisatorischer Maßnahmen verlangt. Mit diesem Begriffspaar werden alle Handlungen erfasst, die dem Ziel der Datenschutzkonformität dienen.[8]

Grundlage ist ein risikobasierter Ansatz. Das Niveau der datenschutzrechtlichen Anforderungen an die Datenschutzmaßnahmen wird dem Risiko angepasst, das von einer Verarbeitung ausgeht. Dabei sind die Anforderungen umso umfangreicher, je größer die Wahrscheinlichkeit und die Schwere einer möglichen Verletzung der Rechte und Freiheiten einer natürlichen Person sind.[9]

Es werden sieben unbestimmte Rechtsbegriffe genannt, die als Faktoren bei der Abwägung geeigneter Maßnahmen berücksichtigt werden müssen. Dies sind Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte sowie Freiheiten natürlicher Personen. Erwägungsgrund 75 der EU-DSGVO versucht diese unbestimmten Rechtsbegriffe mit beispielhaften Aufzählungen für den Rechtsanwender zu konkretisieren. In den Aufzählungen werden scheinbar gleichrangige Punkte genannt, die sich jedoch nicht zu einem einzigen gemeinsamen Oberbegriff zusammenfügen lassen und somit keine Einzelelemente für einen solchen sind. Sie lassen sich jedoch mehreren Oberbegriffen zuordnen, die als Faktoren berücksichtigt werden müssen, und dienen somit als Hilfestellung zur Identifizierung von geeigneten technischen und organisatorischen Maßnahmen. Es handelt sich dabei um die Oberbegriffe Schaden, Risiko, Art der Daten, Umstände der Verarbeitung und Umfang der Verarbeitung. Die Beispiele aus der Auflistung in Erwägungsgrund 75 der EU-DSGVO werden nachfolgend den jeweiligen fünf Oberbegriffen zugeordnet. Für die unbestimmten Rechtsbegriffe „Eintrittswahrscheinlichkeit" und „Zwecke der Verarbeitung" lassen sich in den korrespondierenden Erwägungsgründen keine Beispiele finden.

Schwere der Risiken! Was ist das genau?

Unter dem Begriff „Schwere der Risiken" ist der Schaden oder das Schadenspotenzial zu verstehen. Denkbar sind physische, materielle oder immaterielle Schäden. Für den immateriellen Schaden werden als Beispiele Diskriminierung, Identitätsdiebstahl oder Betrug, Rufschädigung oder erhebliche gesellschaftliche Nachteile

8 Wolf/Brink/*Schmidt/Brink*, Artikel 24 DSGVO, Rn. 12.

9 Paal/Pauly/*Martini*, Artikel 24 DSGVO, Rn. 2.

genannt. Bei einem materiellen Schaden kann es sich um finanzielle Verluste oder erhebliche wirtschaftliche Nachteile handeln.

Risiko! Oder auch nicht!

Es werden beispielhaft (insoweit nicht abschließend) folgende Arten von Risiken aufgeführt:

- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten,
- unbefugte Aufhebung der Pseudonymisierung,
- Einschränkung der Rechte der Betroffenen (Betroffene werden um ihre Rechte und Freiheiten gebracht oder daran gehindert, die sie betreffenden Daten zu kontrollieren).

Art der Daten! Alle diejenigen, um die wir uns besonders sorgen?

Für Datenarten enthält die Aufzählung folgende (nicht abschließende) Beispiele: Daten, aus denen Folgendes hervorgeht:

- die rassische oder ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder
- die Zugehörigkeit zu einer Gewerkschaft.

Weiterhin werden genannt:

- genetische Daten,
- Gesundheitsdaten oder
- das Sexualleben oder
- strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln,
- Daten schutzbedürftiger Personen, insbesondere Daten von Kindern.

Die in Erwägungsgrund 75 EU-DSGVO aufgezählten Datenarten entsprechen dabei denen, die auch in Artikel 9 EU-DSGVO genannt werden. Gemäß Artikel 35 Absatz 3 EU-DSGVO führt eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 EU-DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 EU-DSGVO zur Pflicht, eine DSF durchzuführen.

Umstände der Verarbeitung! Oder Bewertung persönlicher Aspekte?

Zur Konkretisierung des Begriffs „Umstände der Verarbeitung" wird beispielhaft – und damit nicht abschließend – aufgeführt: Die Bewertung persönlicher Aspekte betreffend

- die Arbeitsleistung,
- wirtschaftliche Lage,
- Gesundheit,
- persönliche Vorlieben oder Interessen,
- die Zuverlässigkeit oder das Verhalten,
- den Aufenthaltsort oder Ortswechsel,
- sowie die damit verbundene Analyse oder Prognose, um persönliche Profile zu erstellen oder zu nutzen.

Bei den aufgeführten Umständen der Verarbeitung dürfte es sich um solche handeln, die dazu führen, dass die Analyse des Schutzbedarfs der Datenverarbeitung hoch oder sehr hoch ausfällt. Ergänzend dazu werden in Artikel 35 Absatz 3 EU-DSGVO zwei weitere Beispiele für Verarbeitungsumstände aufgezählt:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen,
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Zu den Umständen der Verarbeitung dürfte auch der in Artikel 35 Absatz 1 EU-DSGVO aufgeführte Fall der Verwendung neuer Technologien zählen.

Umfang der Verarbeitung! Geht es hier um Big Data?

Der Begriff „Umfang der Verarbeitung" wird in den Erwägungsgründen nicht näher ausgeführt. Lediglich ein weniger hilfreiches Beispiel wird in diesem Zusammenhang genannt. Dieses spricht von der Verarbeitung einer großen Menge personenbezogener Daten und einer großen Anzahl von betroffenen Personen. Der Begriff bezieht sich somit – wenig überraschend – auf die Menge der Daten und die Anzahl der betroffenen Personen.

Artikel 25 EU-DSGVO! Oder was ist denn eigentlich privacy by design oder privacy by default?

Artikel 25 EU-DSGVO steht in enger Wechselbeziehung mit Artikel 24 EU-DSGVO. Die Wortwahl der beiden Vorschriften weist eine hohe Schnittmenge auf. Auf den ersten Blick erscheint unklar, wie die Regelungsfelder der Vorschriften abgegrenzt werden können.[10] Artikel 25 EU-DSGVO versteht sich jedoch im Verhältnis beider Vorschriften als Lex specialis. Es handelt sich um eine Konkretisierung im Hinblick auf originäre Datenschutzmaßnahmen, durch die die Rechte der betroffenen Personen geschützt werden sollen. In Absatz 1 der

10 Paal/Pauly/*Martini*, Artikel 24 DSGVO, Rn. 5.

Vorschrift werden die bereits aus dem BDSG (alt) bekannten Maßnahmen der Datenminimierung und Pseudonymisierung genannt. Die bislang eher weniger bekannten Konzepte „Datenschutz durch Technik" (privacy by design) und „Datenschutz durch datenschutzfreundliche Voreinstellungen" (privacy by default) sind zwei weitere prominente Beispielmaßnahmen zur Sicherstellung, dass die Verarbeitungen entsprechend den Vorgaben der Verordnung erfolgt.

Artikel 25 EU-DSGVO ergänzt Artikel 24 EU-DSGVO insoweit, dass die Auswahl geeigneter Maßnahmen verhältnismäßig sein muss. Verantwortlichen wird die Möglichkeit eröffnet, Umstände wie den Stand der Technik und die Implementierungskosten mit den Risiken für die Rechte und Freiheiten natürlicher Personen abzuwägen.

Artikel 32 EU-DSGVO! Reichen sechs Schutzziele aus?

Auch in Artikel 32 EU-DSGVO wird der aus dem BDSG (alt) bekannte Begriff der technischen und organisatorischen Maßnahmen aufgegriffen. Die Anforderungen an die Maßnahmen werden hier vervollständigt. Die Schnittmenge der Wortwahl mit den Artikeln 24 und 25 EU-DSGVO ist erneut auffällig hoch. Nur im Detail ist erkennbar, dass Artikel 32 EU-DSGVO eine andere Zielrichtung verfolgt. Der Fokus liegt auf den klassischen Schutzzielen der IT-Sicherheit. Ziel ist also die Gewährleistung der IT-Sicherheit im engeren Sinn.

Es ist daher folgerichtig, dass Normadressat – anders als bei Artikel 24 EU-DSGVO – neben dem Verantwortlichen auch der Auftragsverarbeiter ist. Ist im Rahmen einer Auftragsverarbeitung zwar der Verantwortliche für die Einhaltung der originären Datenschutzmaßnahmen zuständig, so ist jedoch der Auftragsverarbeiter üblicherweise für die Einhaltung der Datensicherheit und Gewährleistung der klassischen Schutzziele zuständig.

Auch Artikel 32 EU-DSGVO fordert eine Analyse der Risiken, die aus den jeweiligen Prozessen oder Verfahren aus Sicht der Betroffenen hervorgehen können. Wie bereits in den Artikel 24 und 25 EU-DSGVO hat eine Risikoanalyse zu erfolgen, im Rahmen derer Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeiten sowie das Schadenspotenzial berücksichtigt werden sollen. Für fünf dieser sieben unbestimmten Rechtsbegriffe werden in den Erwägungsgründen Beispiele aufgeführt.

Die Unterschiede zu den vorangegangenen Artikeln scheinen zunächst im Detail zu liegen. So wird lediglich bei der Ableitung der Maßnahmen zusätzlich eine Berücksichtigung des Stands der Technik und der Implementierungskosten gefordert. Hieraus sowie aus dem Begriff der „Datensicherheitsrisiken" im korrespondierenden Erwägungsgrund 83 und der Auflistung von Maßnahmen in Artikel 32 Absatz 1 lit. a-d EU-DSGVO geht jedoch hervor, dass die Norm in erster Linie auf die Identifizierung von klassischen IT-Sicherheitsrisiken und deren Vermeidung durch Etablierung technischer Sicherheitsmaßnahmen abzielt – wobei auch Vorgaben gemacht werden, die i.d.R. auf organisatorischer Ebene einzurichten sind (z.B. Pseudonymisierung und ein Verfahren zur regelmäßigen Überprüfung der Maßnahmen).

Sinn und Zweck der Norm geht – anders als der Wortlaut vermuten lässt – aus Artikel 32 Absatz 1 lit. b EU-DSGVO hervor. Danach sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sichergestellt werden. Die Begriffe Systeme und Dienste sind weit auszulegen und können mit Verfahren oder Prozessen gleichgesetzt werden. Die Unterschiede zu Artikel 25 EU-DSGVO sind somit deutlich erkennbar. Während Artikel 25 EU-DSGVO auf die Vermeidung von Datenschutzrisiken im engeren Sinn abzielt – hat Artikel 32 EU-DSGVO die Vermeidung der klassischen IT-Risiken im Sinn. Entsprechend handelt es sich um zwei eigenständige Risikoanalysen, bei denen lediglich die Methodik im weitesten die Gleiche ist.

Abgrenzung zu Artikel 35 EU-DSGVO! Was hat die Datenschutz-Folgenabschätzung (im Folgenden DSF) mit IT-Sicherheit zu tun?

Regelungsinhalt (brauchbarer Natur) oder Unsinn?

Artikel 35 EU-DSGVO hat die DSF zum Inhalt. Hierbei handelt es sich um ein neues Instrument der EU-DSGVO, das jedoch im Kern mit der Vorabkontrolle des Artikel 20 der Richtlinie 95/46/EG bzw. § 4d Absatz 5 BDSG (alt) vergleichbar ist. Doch bereits bei der Frage, wann eine DSF erforderlich ist, weicht der Wortlaut von der bisherigen Regelung im BDSG (alt) ab. Nach dem BDSG (alt) ist objektives Tatbestandsmerkmal, dass eine automatisierte Verarbeitungen vorliegen muss. Diese muss das weitere subjektive Tatbestandsmerkmal der besonderen Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Eine weitere Einschränkung erhält die Vorschrift durch § 4d Absatz 5, 2. Halbsatz BDSG (alt). Danach muss, selbst wenn die ersten beiden Tatbestände erfüllt sind, keine Vorabkontrolle durchgeführt werden, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechts-

geschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Dies hat in der Praxis dazu geführt, dass in den weit überwiegenden Fällen eine Vorabkontrolle gesetzlich nicht verpflichtend war.

Artikel 35 EU-DSGVO verfolgt zwar ebenfalls einen risikobasierten Ansatz; die DSF wird jedoch für alle (nicht nur die automatisierten Datenverarbeitungen) angeordnet. Beschränkt wird die Anordnung nur dadurch, dass die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen nach sich ziehen muss. Eine solche Einschränkung des Anwendungsbereichs erscheint aufgrund des vergleichsweise (hohen) Aufwands angemessen.[11] Im Ergebnis dürfte dies jedoch dazu führen, dass die DSF eine deutlich höhere Relevanz als die Vorabkontrolle erlangt.

Die inhaltlichen Anforderungen an die DSF sind – anders als bei der Vorabkontrolle – sehr deutlich konturiert. Im Grundsatz wird dem Verantwortlichen die Aufgabe zugewiesen, Folgewirkungen sensibler Verarbeitungsprozesse für das Recht der betroffenen Person zu antizipieren.[12]

Im Detail listet Artikel 35 Absatz 7 EU-DSGVO vier Elemente auf, die die DSF zumindest enthalten soll. Diese Elemente finden sich wieder in den verschiedenen Phasen einer DSF, wie sie beispielsweise vom Forum Privatheit[13] empfohlen werden:

- Vorbereitungsphase gemäß Artikel 35 Absatz 7 lit. a EU-DSGVO (systematische Beschreibung, Zwecke, Interessenabwägung),
- Bewertungsphase gemäß Artikel 35 Absatz 7 lit. b u. c EU-DSGVO (Verhältnismäßigkeitsprüfung und Risikoanalyse),
- Maßnahmenphase nach Artikel 35 Absatz 7 lit. d EU-DSGVO (Behandlung und Eindämmung der Risiken),
- Berichtsphase (Dokumentation der Ergebnisse).[14]

Abgrenzung zu anderen Normen! Oder braucht es eine Datenschutz-Folgenabschätzung überhaupt noch?

Fraglich ist, ob bei wortgetreuer Anwendung der Artikel 24, 25 und 32 EU-DSGVO die Durchführung einer DSF hinfällig und Artikel 35 EU-DSGVO somit weitgehend obsolet wäre. Dies wäre dann der Fall, wenn alle Anforderungen aus Artikel 35 EU-DSGVO bereits mit Anwendung der vorgenannten Artikel umgesetzt wären.

Die wesentlichen Anforderungen der DSF ergeben sich aus Artikel 35 Absatz 1 Satz 1 EU-DSGVO. Danach hat eine DSF eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten zum Gegenstand. Eine weitergehende Konkretisierung erfährt die Norm in Absatz 7. Nach Artikel 35 Absatz 7 lit. a EU-DSGVO hat eine DSF eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen zu enthalten. Ähnliche Anforderungen ergeben sich bereits aus den Vorgaben zur Verarbeitungsübersicht bzw. den allgemeinen Dokumentationspflichten im Rahmen der EU-DSGVO. Gleiches gilt für die Vorgabe aus Artikel 35 Absatz 7 lit. b. EU-DSGVO. Die Vorgaben aus Artikel 35 Absatz 7 lit. c und d EU-DSGVO zur Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und Dokumentation von Abhilfemaßnahmen ergeben sich – wie oben ausführlich dargelegt – hingegen bereits aus Artikel 24 und 25 für die originären Datenschutzrisiken bzw. Artikel 32 EU-DSGVO für Datensicherheitsrisiken. Die wesentlichen Inhalte einer DSF werden somit bereits bei wortgetreuer Anwendung der Artikel 24, 25 und 32 EU-DSGVO umgesetzt.

Es stellt sich somit die Frage, wie weitgehend die Pflicht zu Durchführung einer Risikoanalyse ist. Eine systematische Auslegung im Lichte des Artikels 35 EU-DSGVO und insbesondere dessen initialer Anforderung, ob eine Form der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat, führt zu dem Ergebnis, dass die Pflicht zur Durchführung einer Risikoanalyse im Rahmen der Artikel 24, 25 und 32 EU-DSGVO eingeschränkt ausgelegt werden kann. Eine detaillierte Risikoanalyse ist dort demnach nicht zwingend erforderlich. Vielmehr genügt es, diese im Rahmen der DSF durchzuführen. Um dennoch auch bei Verfahren, die kein hohes Risiko zur Folge haben, risikoadäquate technische und organisatorische Maßnahmen auszuwählen und zu beurteilen, ob ein normales oder voraussichtlich hohes Risiko vorliegt, ist die Durchführung einer „kleinen Risikoanalyse“ ausreichend. Wie eine solche aussehen könnte, soll im Folgenden dargestellt werden.

Praktische Umsetzung der IT-Sicherheit! Oder wie wird dies erreicht?

Berücksichtigung bestehender Strukturen!

Aufgrund von Anforderungen aus anderen Bereichen wie beispielweise den Mindestanforderungen an das Risikomanagement (MaRisk) im Finanzsektor finden sich

11 Paal/Pauly/*Martini*, Artikel 35 DSGVO, Rn. 9.

12 Paal/Pauly/*Martini*, Artikel 35 DSGVO, Rn. 3.

13 Vgl. Forum Privatheit, White Paper Datenschutz-Folgenabschätzung, www.forum-privatheit.de/forum-privatheit-de/aktuelles/aktuelles/aktuelles_047.php; Seite vom 6.8.2017.

14 Vgl. Wolff/Brink/*Hansen*, Artikel 35 DSGVO, Rn. 26–35.

in der unternehmerischen Praxis häufig Strukturen und Prozesse, mittels derer IT-Risiken bereits identifiziert und verringert werden können. Hierbei werden beispielsweise zunächst Geschäftsprozesse, IT-Systeme und Anwendungen identifiziert und sodann entsprechende IT-Risiken ermittelt und Maßnahmen abgeleitet.

Es stellt sich die Frage, wie diese bestehenden Strukturen möglichst effizient ausgenutzt werden können, um die zusätzlichen Anforderungen aus der EU-DSGVO hinsichtlich der technischen und organisatorischen Maßnahmen umzusetzen.

Im Folgenden werden die in der Praxis häufig anzutreffenden Vorgehensweisen nach IT-Grundschutz und die Methodik aus dem Standard-Datenschutzmodell (SDM) summarisch vorgestellt. Anschließend wird die praktische Vorgehensweise zur Umsetzung der technischen und organisatorischen Maßnahmen gemäß der EU-DSGVO anhand dieser beiden Standards skizziert.

Geeignete Standards! Sind diese auch anerkannt?

IT-Grundschutz! Ist das nicht zu kompliziert?

Der IT-Grundschutz ist eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Vorgehensweise zum Identifizieren und Umsetzen von Sicherheitsmaßnahmen.[15] Es handelt sich um einen De-Facto-Standard für IT-Sicherheit in Unternehmen und Behörden. Er enthält Empfehlungen zu Methoden, Prozessen, Verfahren und Vorgehensweisen zur Errichtung eines Managementsystems für Informationssicherheit. Weiterer Bestandteil ist das IT-Grundschutz-Kompendium, innerhalb dessen Empfehlungen von Standard-Sicherheitsmaßnahmen gegeben werden. Der IT-Grundschutz basiert auf der Idee und dem Ziel, durch Anwendung der Methodiken aus den Standards und Umsetzung der technischen, infrastrukturellen, organisatorischen sowie personellen Maßnahmen aus dem IT-Grundschutz-Kompendium ein Schutzniveau zu erreichen, das für einen Großteil der IT-Systeme ausreichend ist. Auf eine detaillierte Risikoanalyse und differenzierte Analyse von Schadenshöhen bzw. Eintrittswahrscheinlichkeiten kann dabei – in den meisten Fällen – verzichtet werden. Dies ist auch deshalb sinnvoll, weil insbesondere für die Eintrittswahrscheinlichkeit einer möglichen Beeinträchtigung – schon aufgrund einer fehlenden statistischen Datenbasis – keine exakten Werte angegeben werden können.

Kern der Vorgehensweise nach dem IT-Grundschutz ist daher eine Schutzbedarfsfeststellung. Diese dient der Feststellung, für welche IT-Systeme das etablierte „normale“ Schutzniveau ausreichend ist. Hierzu werden für jede Anwendung und jedes IT-System bzw. die darin verarbeiteten Informationen die zu erwartenden Schäden für das Unternehmen betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können.[16] Auf diese international anerkannten „Grundwerte“ der Vertraulichkeit, Integrität und Verfügbarkeit nimmt nunmehr auch Artikel 32 Abs. 1 lit. b EU-DSGVO Bezug.[17] Der Standard sieht eine Klassifizierung in die Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ vor. Erst bei „hohem“ oder „sehr hohem“ Schutzbedarf ist eine Risikoanalyse durchzuführen.

Standard-Datenschutzmodell! Was haben die Datenschutzaufsichtsbehörden denn damit verzapft?

Im Rahmen der Vorgehensweise nach IT-Grundschutz und insbesondere bei der Durchführung der Schutzbedarfsanalyse wird die Sicht des Betroffenen und sein Schadenspotenzial aufgrund der Datenverarbeitung nur eingeschränkt und damit nicht ausreichend betrachtet, um den Anforderungen der EU-DSGVO zu genügen.

Es lohnt daher ein Blick auf das Standard-Datenschutzmodell (im Folgenden SDM), das in methodischer Analogie zum IT-Grundschutz – von den Datenschutzaufsichtsbehörden – entwickelt worden ist.

Die herkömmlichen Schutzziele der Datensicherheit geben den tatsächlichen Schutzbedarf und die Anforderungen des Datenschutzrechtes nur unzureichend wieder.[18] Kern des SDM ist es daher, die aus der Datensicherheit entspringenden Schutzziele durch „neue Schutzziele“[19] des Datenschutzes sinnvoll zu ergänzen.

Das SDM stellt dazu sechs einheitliche Gewährleistungsziele in den Mittelpunkt. Die ersten drei Schutzziele sind aus der Datensicherheit bekannt. Namentlich handelt es sich um die Verfügbarkeit, Integrität und Vertraulichkeit. Als neue Datenschutzschutzziele werden Transparenz, Nichtverkettbarkeit und Intervenierbarkeit formuliert. Diese Schutzziele stellen letztlich Oberbegriffe für einzelne datenschutzrechtliche Anforderungen des BDSG (alt) bzw. der EU-DSGVO dar. Die Verknüpfung der einzelnen Anforderungen mit den Schutzzielen ist im SDM abgebildet.[20] Damit werden

15 Vgl. www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html, Seite vom 27.12.2017.

16 Vgl. www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Standards/ITGrundschutzStandards_node.html, Seite vom 27.12.2017.

17 Paal/Pauly/*Martini*, Artikel 32 DSGVO, Rn. 58.

18 Wolff/Brink/*Karg*, § 9 BDSG, Rn. 51.

19 *Bock/Rost*, DuD 2011, S. 30 (32).

20 Vgl. www.datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf, Seite vom 28.7.2017.

nicht nur die Anforderungen von Datenschutz sowie Datensicherheit, sondern auch die Vorgaben des BDSG (alt) und der EU-DSGVO miteinander „vereint".

Vorgehensweise in der betrieblichen Praxis! Was genau ist nun umzusetzen?

Informationssicherheitsmanagement (Daten-Sicherheit im engeren Sinne)!

Sofern Unternehmen streng gemäß dem IT-Grundschutz vorgehen oder ihre Prozesse und Strukturen im IT-Sicherheitsbereich mindestens an der Vorgehensweise nach dem IT-Grundschutz ausrichten und somit ein Basisschutzniveau etablieren, werden die Anforderungen des Artikels 32 EU-DSGVO wohl bereits überwiegend erfüllt sein. Allerdings wird im Rahmen des IT-Grundschutzes die Sichtweise des Betroffenen nicht ausreichend gewürdigt. Dies ist jedoch wesentlicher Bestandteil der EU-DSGVO.

Die Vorgehensweise nach IT-Grundschutz ist hinsichtlich der Durchführung der Schutzbedarfsanalyse deshalb (leicht) anzupassen. Zunächst ist die Definition des Schutzziels der Vertraulichkeit auf die Erfüllung aller datenschutzrechtlichen Regelungen aus der EU-DSGVO auszuweiten – sofern personenbezogene Daten verarbeitet werden. Zusätzliche Schutzziele und Bewertungen der Schadenspotenziale bei Verletzung der Schutzziele sind somit (grundsätzlich) nicht erforderlich.

Ergänzend zu der „Unternehmenssichtweise" ist auch – wie bereits erwähnt – die „Betroffenensichtweise" zu betrachten, um das Schadenspotenzial aus Sicht des Betroffenen bei Verletzung des Schutzziels Vertraulichkeit zu bewerten.

Darüber hinaus müssen bei der Feststellung des Schutzbedarfs die Faktoren Verwendung neuer Technologien, Art, Umfang, Umstände und Zwecke der Verarbeitung berücksichtigt werden. Bei der Analyse der Auswirkung der genannten Faktoren auf den Schutzbedarf des Prozesses/Verfahrens oder IT-Systems dürften insbesondere die Ausführungen in den zu Artikel 24 und 25 EU-DSGVO korrespondierenden Erwägungsgründen Hilfestellung bieten.

Eine solche Schutzbedarfsanalyse nach IT-Grundschutz, ergänzt um die Anforderungen aus der EU-DSGVO, kann als „kleine Risikoanalyse" bezeichnet werden, denn die Berücksichtigung der o.g. Faktoren impliziert – jedenfalls eingeschränkt – eine Berücksichtigung von Gefährdungen und Schwachstellen und somit indirekt auch die Bewertung von Eintrittswahrscheinlichkeiten.

Eine solche, (sehr) umfassende Schutzbedarfsstellung enthält bereits Anteile einer komplexeren Risikoanalyse bzw. ist selbst Bestandteil einer solchen. Diese ist im (ersten Schritt) jedoch gerade nicht zwingend erforderlich, sondern erst dann, wenn ein „hoher" oder „sehr hoher" Schutzbedarf festgestellt wurde.

Ist dies der Fall, ist nach der Vorgehensweise des IT-Grundschutzes eine Risikoanalyse durchzuführen. Bei dieser werden Bedrohungen und Schwachstellen in Verbindung mit dem Schadenspotenzial für das Unternehmen bewertet. Auch hier ist dann ergänzend die „Betroffenensichtweise" einzunehmen. Dabei sollten sich die Risiken (an sich) nicht ändern, denn auch die Gefährdungen und Schwachstellen bleiben die gleichen. Lediglich der Schaden bzw. das Schadenspotenzial ist aus Sicht des Betroffenen (unter Umständen) abweichend zu bewerten. Im Ergebnis kann sich somit eine andere Ausprägung des Risikos ergeben. Wer diese Analyse durchführt, ist (grundsätzlich) nicht von Bedeutung. Beispielsweise könnte sie im Rahmen der ohnehin durchzuführenden DSF durch den Verantwortlichen selbst bzw. unterstützend durch den Datenschutzbeauftragten durchgeführt werden.

Datenschutzmanagement (Daten-Schutz im engeren Sinne)

Ähnlich wie für den Bereich der Informationssicherheit muss mittels festgelegter Prozesse und Maßnahmen ein Basisschutzniveau für den Datenschutz erreicht werden. Zwar existieren hier keine Maßnahmenkataloge analog zu den IT-Grundschutz-Katalogen im Bereich IT-Sicherheit, dies ist jedoch nicht (zwingend) erforderlich. Mit dem Baustein „B 1.5 Datenschutz" des IT-Grundschutzes liegt eine geeignete Übersicht der – gemäß dem BDSG (alt) – zu etablierenden, originären Datenschutzmaßnahmen vor. Der Baustein enthält Empfehlungen für eine angemessene Organisation des Datenschutzes im Unternehmen. Darüber hinaus sind Einzelmaßnahmen enthalten. Da die Anforderungen der EU-DSGVO darin nicht berücksichtigt sind, muss vor Verwendung des Bausteins zunächst eine Überarbeitung erfolgen.

Ist ein angemessenes Basisdatenschutzniveau etabliert, kann die im Rahmen der Informationssicherheit (bereits) durchgeführte Schutzbedarfsanalyse verwendet werden. Dadurch kann auch im Datenschutzbereich auf eine detaillierte Risikoanalyse verzichtet werden, sofern es sich um ein „normales" Schutzniveau handelt. Dies ist auch deshalb sinnvoll, weil für die Durchführung einer detaillierten Risikoanalyse i.d.R. keine ausreichende statistische Datenbasis vorliegt, um die Eintrittswahrscheinlichkeiten für Datenschutzrisiken und die Perspektive der betroffenen Person zu bewerten.[21] Im Rahmen der Schutzbedarfsanalyse wird sogleich die Prü-

21 *Bieker/Hansen/Friedwald*, RDV 2016, S. 188 (193).

fung der Relevanzschwelle zur Durchführung einer DSF durchgeführt. Immer dann, wenn bei der Schutzbedarfsanalyse ein „hoher“ oder „sehr hoher“ Schutzbedarf festgestellt wurde, ist eine DSF durchzuführen. Bestandteil einer solchen ist die Analyse von Datenschutzrisiken. Diese ist nicht mit der Risikoanalyse im Bereich IT-Sicherheit zu verwechseln. Zwar kann diese auch Bestandteil der DSF sein, ein Risiko in der Informationssicherheit ist jedoch nicht kongruent mit Datenschutzrisiken. Es müssen daher zusätzlich die Risiken für den Betroffenen bei Verletzung der Schutzziele Transparenz, Nichtverkettbarkeit und Intervenierbarkeit identifiziert werden. Folgerichtig muss auch die verantwortliche Stelle als potenzieller Angreifer bzw. Risikoquelle für Verletzungen der Rechte der betroffenen Personen betrachtet werden. Beispielsweise könnte in diesem Sinne ein Angriff bzw. eine Gefährdung darin bestehen, dass eine Abteilung des Unternehmens eine Nutzung der personenbezogenen Daten zu nicht kompatiblen Zwecken beabsichtigen würde.[22] Insoweit läge eine Verletzung des Schutzziels der Nichtverkettbarkeit vor.

Um abschließend die identifizierten Risiken adäquat zu behandeln, bietet das SDM eine Übersicht generischer Schutzmaßnahmen an, um die jeweils geeigneten Maßnahmen auswählen zu können.[23] Darüber soll vom AK Technik in der Konferenz der unabhängigen Datenschutzbehörden (noch) ein (abschließender) Katalog von Referenzschutzmaßnahmen erarbeitet werden.[24]

Schlussbetrachtung oder auch Fazit!

Mit der EU-DSGVO sind spätestens mit Wirkung vom 25. Mai 2018 neue Verpflichtungen für die Gewährleistung des Datenschutzes und der Datensicherheit umzusetzen. Das übergeordnete Prinzip der Rechenschaftspflicht zwingt Unternehmen, ihre Datenverarbeitungsprozesse nicht nur datenschutzkonform zu gestalten, sondern auch dazu, diese Konformität auch zu dokumentieren und nachzuweisen. Die EU-DSGVO implementiert dabei einen risikobasierten Ansatz für die Umsetzung „technischer und organisatorischer Maßnahmen“, um Datenschutz und Datensicherheit in der Verarbeitung zu erreichen.

Aufgrund der Artikel 24, 25 und 32 EU-DSGVO muss nicht zwingend und in jedem Fall eine detaillierte sowie umfassende Risikobewertung vorgenommen werden. Stattdessen kann ein mehrstufiger Ansatz gewählt werden. Dieser sollte im ersten Schritt vorsehen, dass für die eigenen Prozesse/Verfahren oder Systeme eine „kleine Risikoanalyse“ durchzuführen ist. Dabei würde die aus dem Informationssicherheitsmanagement bekannte Schutzbedarfsanalyse um Aspekte der EU-DSGVO erweitert.

In einem zweiten Schritt sollte die Etablierung eines Basisschutzniveaus in den Bereichen Informationssicherheit (Datensicherheit) und Datenschutz gewährleistet werden. Wie dies im Einzelnen zu geschehen hat, bleibt dem Verantwortlichen für den Datenschutz überlassen. Hierzu kann er sich – nach jetzigem Sach- und Kenntnisstand – verschiedener Modelle bedienen.

Ein etabliertes Schutzniveau – nach welchem Modell auch immer – ermöglicht den Verzicht einer Risikoanalyse für einen Großteil der Prozesse/Verfahren und Systeme. Erst wenn im Rahmen der Schutzbedarfsanalyse ein „hoher“ oder „sehr hoher“ Schutzbedarf festgestellt wird, ist eine Risikoanalyse durchzuführen. Diese kann im Rahmen der DSF erfolgen.

Dieser mehrstufige Ansatz erlaubt es Unternehmen, die vorhandenen Prozesse und Strukturen im Bereich der Informationssicherheit gewinnbringend für den Datenschutz einzusetzen. Durch die Etablierung eines Mindestschutzniveaus kann der Aufwand einer detaillierten Risikoanalyse, so wie sie in den Artikeln 24, 25 und 32 EU-DSGVO dem Wortlaut nach gefordert wird, in vielen Fällen vermieden werden. Dies widerspricht nicht der EU-DSGVO, weil eine Abgrenzung zu einer eventuell aufwändigen DSF weiterhin möglich sein muss. Unternehmen, die sich bislang an keinem Standard orientiert haben, sollten dies angesichts existenzbedrohender Bußgeldrisiken zeitnah nachholen oder andere datenschutzkonforme Lösungsansätze wählen, um ihrer Rechenschaftspflicht nachkommen zu können.

Antonio Ralf W. Reschke ist seit über 25 Jahren als Berater und Rechtsanwalt tätig. Er ist zertifizierter Organisationsberater mit dem Schwerpunkt SAP R/3 (GIBcert)), zertifizierter betrieblicher Datenschutzbeauftragter (GDDcert) sowie behördlich akkreditierter Gutachter für die Anerkennungsbereiche Technik und Recht beim ULD. Er ist langjähriger (Konzern-) Datenschutzbeauftragter bzw. Stellvertreter in namhaften Unternehmensgruppen in Europa und GDD Erfa-Kreis-Leiter Stuttgart.

Maximilian Schmidt ist seit Mai 2013 Mitarbeiter eines Outsourcing-Dienstleisters innerhalb der Genossenschaftlichen Finanzgruppe. Tätig als Berater für Datenschutz, IT-Sicherheitsmanagement und IT-Revision.

22 Vgl. *Bieker/Hansen/Friedwald*, RDV 2016, S. 188 (193).

23 Vgl. *Probst*, DuD 2012 S. 439 (443).

24 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf, Seite vom 27.7.2017.