Thomas Wennemann

TOM und die Datenschutz-Grundverordnung

Eine praktische Umsetzung von technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO

Haben die „Acht Gebote des Datenschutzes" aus dem Bundesdatenschutzgesetz bald ausgedient? Häufig wird die Frage gestellt, welche Maßnahmen für die ab Mai 2018 geltende Datenschutz-Grundverordnung (DS-GVO) im Vergleich zu den auf Basis des bisherigen Bundesdatenschutzgesetzes (BDSG-alt) getroffenen Maßnahmen umgesetzt werden müssen. Diese Frage kann jedoch – ebenso wenig wie bei der Umsetzung nach dem bisherigen Bundesdatenschutzgesetz – nicht pauschal beantwortet werden. Im Folgenden sollen die Anforderungen der Datenschutz-Grundverordnung sowie ein möglicher Lösungsansatz für die Ermittlung der erforderlichen technischen und organisatorischen Maßnahmen aufgezeigt werden.

1 Bisheriger Sachstand

Das Bundesdatenschutzgesetz in seiner derzeitigen Fassung (BDSG-alt) fordert die Umsetzung von Maßnahmen in den Kategorien Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle sowie dem Trennungsgebot (Anlage zu § 9 BDSG-alt). Die Maßnahmen müssen durch die verantwortlichen Stellen sowie Auftragsdatenverarbeiter umgesetzt werden und geeignet sein sowie im Verhältnis zur Art der zu schützenden personenbezogenen Daten stehen (§9 BDSG-alt). Konkrete Maßnahmen werden hierbei nicht vorgegeben. Es gibt lediglich einen Hinweis, dass die Maßnahmen zu den Kategorien Zugangs-, Zugriffs- und Weitergabekontrolle die Verwendung von Verschlüsselungsverfahren nach Stand der Technik sein können (Anlage zu § 9 BDSG-alt).[1]

1 Zu den notwendigen Prüfungsschritten im Einzelnen vgl. *Schultze-Melling*, in: Taeger/Gabel, BDSG, 2. Auflage 2013, § 9, Rn. 39 ff. m. w. Nw.

Thomas Wennemann

IT-Sicherheitsexperte bei der datenschutz nord GmbH.

E-Mail:
twennemann@datenschutz-nord.de

2 Datenschutz-Grundverordnung

In der ab dem 25. Mai 2018 anzuwendenden Datenschutz-Grundverordnung (DS-GVO) finden sich derartige Kategorien von umzusetzenden Maßnahmen allerdings nicht mehr. Vielmehr wird ein dem Risiko angemessenes Schutzniveau in den Vordergrund gestellt und eine entsprechende Einschätzung hierzu vorausgesetzt. Dies wird vor allem auch dadurch deutlich, dass die Gewährleistung einer angemessenen Sicherheit bei der Verarbeitung personenbezogener Daten bereits in den Grundsätzen der Datenschutz-Grundverordnung mit aufgenommen wurde. In Art. 5 Abs. 1 lit. f DS-GVO findet sich hierzu, dass personenbezogene Daten „in einer Weise verarbeitet werden [müssen], die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet […]". Dazu werden zu berücksichtigende *Gefährdungen*:

- unbefugte oder unrechtmäßige Verarbeitung,
- unbeabsichtigter Verlust,
- unbeabsichtigte Zerstörung sowie
- unbeabsichtigte Schädigung

genannt, vor denen ein Schutz durch geeignete technische und organisatorische Maßnahmen erreicht werden muss. Zudem findet sich im zweiten Absatz von Artikel 5 die sog. „Rechenschaftspflicht", durch die eine Dokumentation und der Nachweis der getroffenen Maßnahmen notwendig wird (Art. 5 Abs. 2 i.V.m Abs. 1 lit. f DS-GVO). In weiteren Artikeln der Datenschutz-Grundverordnung wird die Umsetzung dieser Grundsätze teilweise noch weiter ausgeführt oder aber vorausgesetzt (z. B. Dokumentation). Dabei stellt sich die Frage, wie überhaupt eine angemessene Sicherheit der personenbezogenen Daten festgestellt und deren Nachweis im Sinne der Rechenschaftspflicht vorgenommen

werden kann.[2] Eine Umsetzungsmöglichkeit dieser Pflichten ist Gegenstand dieses Beitrages und soll im Folgenden näher vorgestellt werden (vgl. 4. Umsetzung).

3 Vorgaben der DS-GVO

Im Folgenden sollen zunächst die relevanten Rechtsvorschriften, aus denen sich Verpflichtungen zur Umsetzung von technischen und organisatorischen Maßnahmen ergeben, übersichtsweise dargestellt werden.[3]

Im ersten Absatz von Art. 24 DS-GVO (Verantwortung des für die Verarbeitung Verantwortlichen) wird zunächst einmal verlangt, dass der Verantwortliche unter Berücksichtigung:

- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und
- Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen

geeignete technische und organisatorische Maßnahmen umsetzt. Der Verantwortliche muss sicherstellen und den Nachweis darüber erbringen können, dass die Verarbeitung gemäß der Datenschutz-Grundverordnung erfolgt und dass die Maßnahmen überprüft und aktualisiert werden (Art. 24 Abs. 1 DS-GVO). Für Auftragsverarbeiter ergibt sich das Erfordernis zum Nachweis der Einhaltung der erforderlichen Maßnahmen (i. S, d. Art. 32 DS-GVO) demgegenüber aus Art. 28 DS-GVO (Art. 28 Abs. 3 lit. h i.V.m. lit. c DS-GVO).

Darüber hinaus wird im Rahmen eines nach Art. 30 DS-GVO notwendigen Verzeichnisses der Verarbeitungstätigkeiten,– wenn möglich – von den Auftragsverarbeitern und Verantwortlichen eine allgemeine Beschreibung der im Sinne von Art. 32 DS-GVO getroffenen Maßnahmen gefordert (Art. 30 Abs. 1 lit. g und Abs. 2 lit. d i.V.m. Abs. 3 DS-GVO). Zur Einschränkung, in welchen Fällen diese Verpflichtung nicht besteht, weil sie nicht möglich ist, finden sich hingegen keine Hinweise.

Gemäß Art. 32 Abs. 1 DS-GVO (Sicherheit der Verarbeitung) besteht außerdem die Verpflichtung, dass Verantwortliche und Auftragsverarbeiter unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und
- Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Maßnahmen schließen unter anderem Folgendes ein:

2 Dazu auch *Jandt*, in: Kühling/Buchner, DS-GVO, 2017, Art. 32, Rn. 5 f.

3 Auf die Darstellung des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gem. Art. 25 DS-GVO wird aufgrund des Umfangs nicht eingegangen.

- die Pseudonymisierung und die Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DS-GVO);
- die dauerhafte Sicherstellung von
- Vertraulichkeit,
- Integrität,
- Verfügbarkeit und Belastbarkeit[4] (engl. resilience) (Art. 32 Abs. 1 lit. b DS-GVO);
- die Fähigkeit, Verfügbarkeit und Zugang zu den Daten nach einem Zwischenfall rasch wiederherstellen zu können (engl. restore) (Art. 32 Abs. 1 lit. c DS-GVO);
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit (Art. 32. Abs. 1 lit. d DS-GVO).

Die in Art. 32 Abs. 1 lit. b DS-GVO genannten Begriffe Integrität und Vertraulichkeit sind bereits aus Artikel 5 bekannt und werden durch „Verfügbarkeit und Belastbarkeit" erweitert. Diese übergeordnet erscheinenden Ziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit lassen sich jedoch nicht als direkte Forderungen konkreter Maßnahmen einordnen und werden daher im Folgenden als *Sicherheitsziele* bezeichnet, welche mit den umzusetzenden Maßnahmen auf Dauer sicherzustellen sind.

Die Wiederherstellbarkeit nach einem Zwischenfall und die regelmäßige Überprüfung sind zwar übergreifend umzusetzen, sie stellen jedoch keine eigenen übergreifenden *Sicherheitsziele* dar. Sie verlangen bereits die konkretisierte Umsetzung von Maßnahmen. Entsprechend werden diese nachfolgend als *konkrete Maßnahmenforderungen* bezeichnet.

Im zweiten Absatz des Art. 32 DS-GVO werden zudem die mit der Verarbeitung verbundene Risiken benannt:

- unbeabsichtigte/unrechtmäßige Vernichtung (engl. destruction),
- unbeabsichtigter/unrechtmäßiger Verlust (engl. loss),
- unbeabsichtigte/unrechtmäßige Veränderung (engl. alteration),
- unbefugte Offenlegung (engl. disclosure) sowie
- unbefugter Zugang (engl. access).

Diese Liste ist jedoch nicht abschließend und erforderlichenfalls entsprechend zu erweitern. Wie diese bei der Beurteilung eines angemessenen Schutzniveaus berücksichtigt werden sollen, wird in der Datenschutz-Grundverordnung nicht näher benannt. Aus diesem Grund erscheint es zunächst erforderlich, den *Schutzbedarf* der verarbeiteten Daten festzustellen. Dieser hängt von den Risiken für die Rechte und Freiheiten natürlicher Personen ab. Die in Art. 32 Abs. 2 DS-GVO gelisteten Punkte stellen daher zu berücksichtigende *Gefährdungen* dar, die abhängig von Art, Umfang, Umständen und den Zwecken der Verarbeitung sowie den getroffenen technischen und organisatorischen Maßnahmen unterschiedlich stark sein können, auf die Datenverarbeitung wirken und den jeweils einschlägigen *Sicherheitszielen* entgegenstehen. Diese mit der Verarbeitung verbundenen Risiken werden daher zum besseren Verständnis im Folgenden als *Gefährdungen* bezeichnet.

Die in Art. 32 Abs. 3 DS-GVO genannten genehmigten Verhaltensregeln und Zertifizierungen stellen überdies weitere Faktoren dar, die als Indizien für die Eignung getroffener Maßnahmen herangezogen werden können.

Eine weitere *konkrete Maßnahmenforderung* folgt in Art. 32 Abs. 4 DS-GVO, welche verlangt, dass die Verarbeitung personenbezogener Daten nur auf Anweisung erfolgt.

4 Umsetzung

Bei der Ermittlung geeigneter technischer und organisatorischer Maßnahmen kann es insbesondere

- aufgrund von unterschiedlichen Arten, Umfängen, Umständen und Zwecken der einzelnen Verarbeitungstätigkeiten sowie
- möglicher unterschiedlicher Schutzbedarfe der verarbeiteten Daten und
- etwaiger unterschiedlicher mit der Verarbeitung verbundenen Gefährdungen und Eintrittswahrscheinlichkeiten

erforderlich sein, die Risiken je Verarbeitungstätigkeit sicherstellen und belegen zu können.

In der praktischen Umsetzung kann eine tabellarische Auflistung hilfreich sein, mit der die Anforderungen strukturiert durchgearbeitet werden können. Hierdurch soll sichergestellt werden, dass sämtliche relevanten Faktoren systematisch erfasst und eine darauf basierende Bewertung der Sicherheit der Verarbeitung personenbezogener Daten erfolgen kann. Zur Struktur der ersten Tabelle werden (vgl. Tabelle 1) folgende Spalten vorgesehen und im Folgenden erläutert:

- Verarbeitungstätigkeit,
- Sicherheitsziele,
- Gefährdungen bei der Verarbeitung,
- Schutzbedarf,
- Begründung zum Schutzbedarf,
- Geeignete getroffene Maßnahmen unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowie ggfs. genehmigter Verhaltensregeln und/oder Zertifizierungen,
- Eintrittswahrscheinlichkeit der Gefährdung unter Berücksichtigung der getroffenen Maßnahmen,
- Begründung zur Eintrittswahrscheinlichkeit,
- Risikowert.

Tabelle 1 |

Verarbeitungstätigkeit	Sicherheitsziele	Gefährdungen bei der Verarbeitung	Schutzbedarf	Begründung zum Schutzbedarf	Geeignete getroffene Maßnahmen unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowie ggfs. genehmigter Verhaltensregeln und/oder Zertifizierungen	Eintrittswahrscheinlichkeit der Gefährdungen unter Berücksichtigung der getroffenen Maßnahmen	Begründung zur Eintrittswahrscheinlichkeit	Risikowert

Die Verarbeitungstätigkeiten können dabei in der entsprechend benannten Spalte aufgeführt werden, wobei die Möglichkeit besteht, auf ein Verzeichnis der Verarbeitungstätigkeiten zu referenzieren. Hierdurch soll erreicht werden, dass Art, Umfang, Umstände und der Zwecke der Verarbeitungen berücksichtigt werden (Art. 32 Abs. 1 DS-GVO). Für jede Verarbeitungstätigkeit

4 Informationen zum Thema „Was ist Belastbarkeit im Sinne von Art. 32 DSGVO?" unter https://www.datenschutz-notizen.de/was-ist-belastbarkeit-im-sinne-von-art-32-dsgvo-3319778/ (Abruf 23.1.2018).

werden die *Sicherheitsziele* aus Art. 32 Abs. 1 lit. b DS-GVO einzeln betrachtet und entsprechend in mehreren Zeilen aufgeführt. Diesen werden den jeweils einschlägigen *Gefährdungen* (insbesondere zu berücksichtigende Risiken der Verarbeitung aus Art. 32 Abs. 2 DS-GVO) zugeordnet.

Der *Schutzbedarf* der verarbeiteten Daten (Berücksichtigung der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen gem. Art. 32 Abs. 1 DS-GVO) ist unter Berücksichtigung der Verarbeitungstätigkeit und der *Sicherheitsziele* festzulegen. Die zur Einschätzung des *Schutzbedarfes* verwendeten Werte sollten definiert und in der entsprechenden Spalte eingetragen werden. Um der Rechenschaftspflicht aus Art. 5 Abs. 2 i. V. m Abs. 1 lit. f DS-GVO nachzukommen, sollten die auf dieser Basis getroffenen Einschätzungen des *Schutzbedarfes* in der Spalte „Begründung zum Schutzbedarf" dokumentiert werden.

In der anschließenden Spalte werden die geeigneten getroffenen Maßnahmen unter Berücksichtigung des Stands der Technik und der Implementierungskosten (Art. 32 Abs. 1 DS-GVO) sowie ggfs. genehmigter Verhaltensregeln und/oder Zertifizierungen (Art. 32 Abs. 3 DS-GVO), welche auf die identifizierten *Gefährdungen* der zu gewährleistenden *Sicherheitsziele* wirken, erfasst. Dabei zu berücksichtigen sind Maßnahmen zur Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO). Für die *Konkreten Maßnahmenempfehlungen*:

- Wiederherstellung, Verfügbarkeit und Zugang nach Zwischenfall (Art. 32 Abs. 1 lit. c DS-GVO),
- regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit (Art. 32 Abs. 1 lit. d DS-GVO) und
- Verarbeitung nur auf Anweisung (Art. 32 Abs. 4 DS-GVO)

kann eine weitere Tabelle angelegt werden, in der die Umsetzung je Verarbeitungstätigkeit erfasst wird. Zwar könnten diese auch den jeweiligen *Sicherheitszielen* zugeordnet werden, ein Mehrwert wäre jedoch fraglich, da die Maßnahmenforderungen *sicherheitszielübergreifend* umzusetzen sind. Auf diese Weise lassen sich Redundanzen bei der Erfassung vermeiden.

In der nächsten Spalte erfolgt nun eine Einschätzung der Eintrittswahrscheinlichkeit der *Gefährdung* unter Berücksichtigung der getroffenen Maßnahmen (Art. 32 Abs. 1 DS-GVO) sowie den Umsetzungen zu den k*onkreten Maßnahmenempfehlungen*. Die getroffenen Maßnahmen sollten geeignet sein, um den identifizierten *Gefährdungen* in ausreichender Weise entgegenzuwirken und damit die *Sicherheitsziele* auf Dauer sicherzustellen (Art. 32 Abs. 2 DS-GVO). Zur objektiven und nachvollziehbaren Bewertung der Eintrittswahrscheinlichkeiten sollten entsprechende Definitionen erstellt werden. Die getroffenen Einschätzungen sollten dann aufgrund der Rechenschaftspflicht in der Spalte „Begründung zur Eintrittswahrscheinlichkeit" dokumentiert werden.

Die Spalte „Risikowert" kann einen Wert enthalten, welcher sich beispielsweise als Produkt der Werte für *Schutzbedarf* und Eintrittswahrscheinlichkeit ergibt.

Es sollte definiert und dokumentiert werden, in welchen Wertebereichen ein angemessenes Schutzniveau angenommen wird, in welchen Wertebereichen die Umsetzungen weiterer Maßnahmen erforderlich sind und ob bei einem identifizierten hohen Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen die Durchführung einer Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO erforderlich sein könnte.

Anhand des ermittelten Risikowertes und den Definitionen könnte so festgestellt und gleichzeitig dokumentiert werden, ob ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 Abs. 1 DS-GVO besteht oder weitere Maßnahmen erforderlich sind, um dieses Niveau zu erreichen.

5 Fazit

Dass die Auswahl der umzusetzenden Maßnahmen nicht mehr wie im Bundesdatenschutzgesetz (BDSG-alt) von einer Liste mit Maßnahmenforderungen abhängt, sondern es vielmehr auf die mit einer Datenverarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen ankommt, wird in der Praxis vielfach als Herausforderung gesehen. Die technischen und organisatorischen Maßnahmen müssen zur Umsetzung der Datenschutz-Grundverordnung nicht neu erfunden werden, jedoch verlangt die Datenschutz-Grundverordnung mehr als ein bloßes Mapping zu den aufgrund des alten Bundesdatenschutzgesetzes getroffenen Maßnahmen.

Im Fokus für die Umsetzung erforderlicher und geeigneter Maßnahmen steht der risikobasierte Ansatz, welcher sich auch in der Informationssicherheit und damit verbundenen Normen, wie bspw. der ISO 27000er Familie, etabliert hat. Im Idealfall wäre das Ergebnis der risikoorientierten Betrachtung, dass mit den bereits getroffenen Maßnahmen ein angemessenes Schutzniveau gewährleistet wird. Andernfalls sind entsprechende Maßnahmen umzusetzen, die auf die identifizierten, einschlägigen *Gefährdungen* wirken. Mithilfe dieser exemplarisch beschriebenen Vorgehensweise sollte es bei regelmäßiger Durchführung möglich sein, die Anforderungen des Art. 32 DS-GVO und die Dokumentations- und Nachweispflichten entsprechend der Datenschutz-Grundverordnung umzusetzen.