Sachstand

„Technische und organisatorische Maßnahmen“

„Technische und organisatorische Maßnahmen“

Aktenzeichen:	WD 3 - 3000 - 126/19
Abschluss der Arbeit:	24. Mai 2019
Fachbereich:	WD 3: Verfassung und Verwaltung

1. Einleitung

Der Sachstand widmet sich der Fragestellung, welche Anforderungen unter die „technischen und organisatorischen Maßnahmen“ im Sinne der Datenschutz-Grundverordnung (DSGVO) fallen und inwieweit diese Anforderungen Niederschlag im neuen Bundesdatenschutzgesetz (BDSG) gefunden haben.

2. Begriffsdefinition „technische und organisatorische Maßnahmen“

Die Begriffe waren bereits in § 9 BDSG a.F. enthalten. Vorgaben für „technische und organisatorische Maßnahmen“ sind nunmehr in vielerlei Artikeln der DSGVO enthalten. Entsprechende Regelungen finden sich insbesondere in:

- Art. 5 Abs. 1 lit. f (Grundsatz der Integrität und Vertraulichkeit);
- Art. 24 Abs. 1 S. 1 (Allgemeine Pflichten des Verantwortlichen);
- Art. 25 Abs. 1 und Abs. 2 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen);
- Art. 28 Abs. 1 (Anforderungen an Auftragsverarbeiter);
- Art. 32 Abs. 1 (Sicherheit der Verarbeitung);
- Art. 34 Abs. 3 (Ausnahme von der Benachrichtigungspflicht);
- Art. 89 Abs. 1 S. 2. (Datenverarbeitung für bestimmte privilegierte Zwecke).

Technische und organisatorische Maßnahmen sind alle erforderlichen Maßnahmen, um die Beachtung des Datenschutzes und der Datensicherheit bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten und den dazu betriebenen Verfahren zu gewährleisten.[1] Der 78. Erwägungsgrund DSGVO sieht vor, dass der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen sollte, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.

Die Differenzierung zwischen technischen und organisatorischen Maßnahmen ist nicht trennscharf möglich. Zu den **technischen Maßnahmen** zählen solche, die sich auf den Datenverarbeitungsvorgang an sich erstrecken (z. B. Zugriffskontrolle, Weitergabekontrolle, Verschlüsselung). **Organisatorische Maßnahmen** beziehen sich dagegen eher auf den äußeren Ablauf der Datenverarbeitung (z. B. Protokollierung, Schulungen der Mitarbeiter, Vieraugenprinzip).[2]

---

1 Schmidt/Brink, in: Wolf/Brink, Datenschutzrecht, 27. Ed., 1.5.2018, Art. 24 DSGVO Rn. 12.

2 Schmidt/Brink, in: Wolf/Brink, Datenschutzrecht, 27. Ed., 1.5.2018, Art. 24 DSGVO Rn. 15.

Technische und organisatorische Maßnahmen könnten nach der beispielhaften **Aufzählung** im **78. Erwägungsgrund** zur DSGVO unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern.

2.1. Art. 32 Abs.1 DSGVO

Im Folgenden werden anhand von Art. 32 Abs. 1 DSGVO die Anforderungen an technische und organisatorische Maßnahmen erläutert. Art. 32 Abs. 1 DSGVO normiert für den Verantwortlichen sowie für den Auftragsverarbeiter allgemein die Pflicht, die geeigneten technischen und organisatorischen Maßnahmen zu treffen, um die Sicherheit der Datenverarbeitung zu gewährleisten.

2.1.1. Kriterien bei der Auswahl der geeigneten Maßnahmen

Nach Art. 32 Abs. 1 DSGVO sind diejenigen Maßnahmen zu treffen, die unter Berücksichtigung von bestimmten Kriterien geeignet sind, ein dem Risiko angemessenes Schutzniveau gewährleisten sollen. Diese aufgezählten Kriterien sind:

- Stand der Technik;
- Implementierungskosten;
- Art, Umfang, Umstände und Zwecke der Datenverarbeitung;
- die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.[3]

Der Begriff der **Geeignetheit** ist nicht im Sinne einer Einschränkung auf bestimmte Maßnahmen zu verstehen. Zur Bestimmung der geeigneten Maßnahmen legt die DSGVO fest, dass diese ein dem Risiko der Verarbeitung angemessenes Schutzniveau bieten müssen. Hierzu ist eine Gesamtabwägung anzustellen, die die Art der zu schützenden Daten, den Stand der Technik sowie die entstehenden Kosten einbezieht.[4] Die Maßnahmen müssen umso wirksamer sein, je höher die drohenden Schäden sind.[5]

Darüber hinaus verlangt Art. 32 Abs. 1 DSGVO, dass das Schutzniveau unter anderem unter Berücksichtigung des **Stands der Technik** und der **Implementierungskosten** sicherzustellen ist. Begrifflich wird der Stand der Technik zwar nicht näher definiert. Gemeint dürften aber technische Maßnahmen sein, die bereits zur Verfügung stehen und die sich zur Erreichung eines bestimmten

3 Vgl. umfassend hierzu: Martini, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 32 DSGVO Rn. 50 ff.

4 Martini, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 32 DSGVO Rn. 26.

5 Hladjik, in: Ehmann/Selmayr, 2. Auflage 2018, Art. 32 DSGVO Rn. 4.

Sicherheitsniveaus bereits entsprechend bewährt haben. Mit dem Erfordernis geht jedoch keine Pflicht einher, neue Techniken zu entwickeln bzw. eine solche Entwicklung abzuwarten.[6]

Art. 32 Abs. 1 DSGVO geht zudem davon aus, dass ein **angemessenes Schutzniveau** zu gewährleisten ist. Der Formulierung ist eine **dauerhafte Pflicht** des Verantwortlichen zu entnehmen. Technische und organisatorische Maßnahmen sind nicht einmalig zu ergreifen, sondern dauerhaft zu überprüfen und ggf. neuen Entwicklungen anzupassen.[7] Der Verweis auf die Implementierungskosten begrenzt jedoch die Pflicht zur Ergreifung entsprechender Maßnahmen auf ein angemessenes Niveau.[8]

2.1.2. Katalog möglicher Maßnahmen

Art. 32 Abs. 1 DS-GVO enthält eine nicht abschließende Auflistung[9] von vier Beispielmaßnahmen:[10]

- Pseudonymisierung und Verschlüsselung (lit. a);
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (lit. b);
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (lit. c);
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (lit. d).

3. Niederschlag der Sicherheitsanforderungen an die Datenverarbeitung im neuen Bundesdatenschutzgesetz

Im neuen Bundesdatenschutzgesetz wurde mit dem § 64 BDSG nahezu wortgleich die Vorgabe des Art. 29 Abs. 1 der JI-Richtlinie (RL EU 2016/680) umgesetzt, welcher seinerseits wiederum dem Grundsatz des Art. 32 Abs. 1 DS-GVO entspricht.[11] Die Norm des § 64 BDSG ähnelt der früheren Regelung in § 9 BDSG a.F., die bereits Vorgaben für technische und organisatorische Maßnahmen

---

6 Hladjik, in: Ehmann/Selmayr, 2. Auflage, 2018, Art. 32 DSGVO Rn. 5.

7 Hladjik, in: Ehmann/Selmayr, 2. Auflage, 2018, Art. 32 DSGVO Rn. 5.

8 Martini, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 32 DSGVO Rn. 60.

9 Vgl. umfassend hierzu: Hladjik, in: Ehmann/Selmayr, 2. Auflage 2018, Art. 32 DSGVO Rn. 6.

10 Vgl. zu den einzelnen Maßnahmen im Detail: Martini, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 32 DSGVO Rn. 30 ff.

11 Schwichtenberg, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage, 2018 § 64 BDSG Rn. 2.

enthielt. Die Inhalte des Art. 32 Abs. 1 lit. a bis c DSGVO wurden in § 64 Abs. 2 BDSG aufgenommen.[12] § 64 BDSG verpflichtet den Verantwortlichen, bei Datenverarbeitungen zu Zwecken der JI-Richtlinie (RL EU 2016/680) erforderliche technisch-organisatorische Maßnahmen zu treffen. Gleichzeitig wird klarstellend geregelt, dass die Ausgestaltung der Maßnahmen Ergebnis eines Abwägungsprozesses sein soll, in den insbesondere der Stand der verfügbaren Technik, die Implementierungskosten, die näheren Umstände der Verarbeitung und die in Aussicht zu nehmende Gefährdung für die Rechtsgüter der betroffenen Person einzustellen sind. Weiterhin wird normiert und damit klargestellt, dass bei der Festlegung der technisch-organisatorischen Maßnahmen die einschlägigen Standards und Empfehlungen, insbesondere Technische Richtlinien, des Bundesamts für Sicherheit in der Informationstechnik zu berücksichtigen sind.[13]

Darüber hinaus sind technisch organisatorische Pflichten an weiteren Stellen des BDSG verankert. Entsprechende Regelungen finden sich in:

- § 22 Abs. 2 Nr. 1 (Verarbeitung besonderer Kategorien personenbezogener Daten);
- § 34 Abs. 1 Nr. 2 (Ausnahme vom Auskunftsrecht der betroffenen Person);
- § 47 Nr. 6 (Allgemeine Grundsätze für die Verarbeitung);
- § 57 Abs. 2 (Ausnahme vom Auskunftsrecht);
- § 71 Abs. 2 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen).

***

12 Gräber/Nolden, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, § 64 BDSG Rn. 5.

13 Vgl. BT-Drs. 18/11325, S. 116.