Das Standard-Datenschutzmodell der Aufsichtsbehörden

Einleitung

Bei einer generellen Überprüfung der datenschutzrechtlichen Vorgaben, sind eine Vielzahl von Einzelnormen zu berücksichtigen, aus denen sich jeweils konkrete Anforderungen für die Verarbeitungsaktivitäten ableiten lassen. Zahlreiche Normen definieren dabei nur abstrakte Vorgaben, die dann in der konkreten Situation interpretiert werden müssen. Die verantwortliche Stelle muss etwa gem. Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen treffen, mit denen die Risiken für die Rechte und Freiheiten natürlicher Personen gemindert werden können. Daneben gelten weitere Grundsätze wie der Grundsatz der Datenminimierung und der Grundsatz der Verhältnismäßigkeit. Konkrete Vorgaben dazu, welche Schutzmaßnahmen getroffen werden müssen und wie die datenschutzrechtlichen Prinzipien umgesetzt werden können, enthält die DSGVO nicht. Die zutreffende Interpretation der Datenschutz-Grundsätze in der DSGVO, also die Subsumtion unter den Verordnungstext, ist deswegen insbesondere für juristische Laien vielfach nur schwer nachzuvollziehen.

Das Standard-Datenschutzmodells der Datenschutzaufsichtsbehörden der Länder und des Bundes („Datenschutzkonferenz" bzw. „DSK") soll den Einstieg in die Thematik erleichtern und die abstrakten Anforderungen der DSGVO in konkrete Schutzmaßnahmen überführen. Nach dem Ziel der DSK soll das Datenschutzrecht damit leichter verstanden und angewendet werden können.

Eine erste Version des Standard-Datenschutzmodell wurde im November 2016 veröffentlicht (V1.0) und im April 2018 leicht überarbeitet; im letzten Monat ist dann die umfassend überarbeitete Version (V2.0) vorgelegt worden.

Wie funktioniert das Datenschutzmodell?

Im Rahmen des Datenschutzmodells werden die verschiedenen rechtlichen Anforderungen der DSGVO bestimmten Schutzzielen zugeordnet. Diese Schutzziele sind:

- Datenminimierung
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Nichtverkettung
- Transparenz
- Intervenierbarkeit

Der Grundgedanke ist, dass sich nahezu alle Anforderungen der DSGVO innerhalb der Schutzziele zusammenfassen lassen. Für jedes Schutzziel werden zugleich bestimmte Schutzmaßnahmen beschrieben, die zur Erreichung des Schutzziels und somit zur Erfüllung der rechtlichen Anforderung beitragen. Typische Maßnahmen zur Erfüllung des Schutzziels „Vertraulichkeit" soll beispielsweise die Festlegung und Umsetzung eines Rechte- und Zugriffskonzepts in einem IT-System sein. Die von der Aufsichtsbehörde berücksichtigten rechtlichen Anforderungen lassen sich wie folgt den verschiedenen Schutzzielen zuordnen:

Schutzziel	**Datenschutzrechtliche Anforderung**
Datenminimierung Schutzziel 1	Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO) Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) Evaluierbarkeit (Art. 32 Abs. 1 lit. d) DSGVO)
Verfügbarkeit Schutzziel 2	Verfügbarkeit (Art. 32 Abs. 1 lit. b) DSGVO) Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO) Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b) und c) DSGVO) Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d), 34 Abs. 2 DSGVO) Evaluierbarkeit (Art. 32 Abs. 1 lit. d) DSGVO)

Integrität Schutzziel 3	Richtigkeit (Art. 5 Abs. 1 lit. d) DSGVO) Integrität (Art. 5 Abs. 1 lit. f), Art. 32 Abs. 1 lit. b) DSGVO) Fehler- und Diskriminierungsfreiheit beim Profiling (Art. 22 Abs. 3, 4 DSGVO i. V. m. ErwGr. 71) Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO) Überwachung der Verarbeitung (Art. 33 DSGVO) Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d), 34 Abs. 2 DSGVO) Evaluierbarkeit (Art. 32 Abs. 1 lit. d) DSGVO)
Vertraulichkeit Schutzziel 4	Vertraulichkeit (Art. 5 Abs. 1 lit. f), Art. 28 Abs. 3 lit. b), Art. 29, Art. 32 Abs. 1 lit. b), Art. 32 Abs. 4, Art. 38 Abs. 5 DSGVO) Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO) Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d), 34 Abs. 2 DSGVO). Evaluierbarkeit (Art. 32 Abs. 1 lit. d) DS-GVO)
Nichtverkettung Schutzziel 5	Zweckbindung (Art. 5 Abs. 1 lit. b) DSGVO) Evaluierbarkeit (Art. 32 Abs. 1 lit. d) DS-GVO)
Transparenz Schutzziel 6	Transparenz für Betroffene (Art. 5 Abs. 1 lit. a), Art. 12 - 15, Art. 34 DSGVO) Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2, Art. 7 Abs. 1, Art. 24 Abs. 1, Art 28 Abs. 3 lit. a), Art. 30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a) und e) DSGVO) Überwachung der Verarbeitung (Art. 33 DSGVO) Einwilligungsmanagement (Art. 4 Nr. 11, Art. 7 Abs. 4 DSGVO) Evaluierbarkeit (Art. 32 Abs. 1 lit. d DS-GVO)
Intervenierbarkeit Schutzziel 7	Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12 Abs. 2 DSGVO) Identifizierung und Authentifizierung (Art. 12 Abs. 6 DSGVO) Berichtigungsmöglichkeit von Daten (Art. 5 lit. d), Art. 16 DSGVO) Löschbarkeit von Daten (Art. 17 Abs. 1 DSGVO) Einschränkbarkeit der Verarbeitung von Daten (Art. 18 DSGVO) Datenübertragbarkeit (Art. 20 Abs. 1 DSGVO) Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen (Art. 22 Abs. 3 DSGVO) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) Einwilligungsmanagement (Art. 4 Nr. 11, Art. 7 Abs. 4 DS-GVO) Umsetzung aufsichtsbehördlicher Anordnungen (Art. 58 Abs. 2 lit. f) und j) DSGVO) Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d), 34 Abs. 2 DSGVO). Evaluierbarkeit (Art. 32 Abs. 1 lit. d) DSGVO)

Der Konzeption des Datenschutzmodells liegt der Gedanke zugrunde, dass mit einzelnen Schutzmaßnahmen zugleich mehrere datenschutzrechtliche Anforderungen umgesetzt werden können. Durch den Fokus auf die Umsetzung der Schutzziele lassen sich nach Auffassung der DSK die zahlreichen rechtlichen Anforderungen bündeln und auch für juristische Laien handhabbarer machen.

Welche konkreten Schutzmaßnahmen beinhaltet das Datenschutzmodell?

In Teil D des Standard-Datenschutzmodells finden sich diverse „generische Maßnahmen", die zur Einhaltung des Datenschutzes innerhalb der verschiedenen Schutzziele beitragen können. Diese Maßnahmen stellen aber nur Beispielmaßnahmen dar und sollen durch konkrete Referenzmaßnahmen im Anhang des Datenschutz-Modells konkretisiert werden. Nach der Konzeption des Standard-Datenschutzmodells sind diese Referenzmaßnahmen von den Aufsichtsbehörden getestet und im Hinblick auf ihre „Praxistauglichkeit erprobt".

Gegenwärtig ist der Anhang E6 des Standard-Datenschutzmodells, der diese Referenzmaßnahmen enthalten soll, allerdings noch leer. Es findet sich lediglich ein Hinweis, dass der Referenzmaßnahmenkatalog „künftig Bestandteil des Standard-Datenschutzmodells" wird. Weiter heißt es: „Dieser Katalog von Bausteinen befindet sich in der Entwicklungs- und Abstimmungsphase und wird ständig weiterentwickelt".

Bewertung und Fazit

Zum gegenwärtigen Zeitpunkt wird das Standard-Datenschutzmodell seinen eigenen Zielen nicht gerecht. Es ist immerhin der selbsterklärte Hauptzweck des Standard-Datenschutzmodells, dass dem juristischen Laien die Interpretation von auslegungsbedürftigen Rechtsbegriffen erspart werden soll. Die Verdichtung der zahlreichen datenschutzrechtlichen Grundsätze und Anforderungen auf wenige Schutzziele mag systematisch noch nachvollziehbar sein. Diese Bündelung bietet aber nur dann einen Mehrwert, wenn sie von konkreten Schutzmaßnahmen begleitet wird. Ohne die konkreten Schutzmaßnahmen im Anhang des Standard-Datenschutzmodells fehlt die von dem Nutzer benötigte Handreichung, wie die Schutzziele konkret beachtet werden sollen. An die Stelle der auslegungsbedürftigen Rechtsbegriffe treten somit auslegungsbedürftige Schutzziele. Versucht sich der Nutzer unterdessen mit dem Inhalt der Schutzziele zu beschäftigen, führt dies zum gegenwärtigen Zeitpunkt zurück zu den allgemeinen datenschutzrechtlichen Grundlagen und dem Wortlaut der DSGVO. Letztlich hat der Nutzer damit nichts gewonnen, sondern muss vielmehr gedanklich einen „weiteren Schritt" vom Schutzziel zur DSGVO-Anforderung tätigen.

Zudem besteht durch die Fokussierung auf Schutzziele eine weitere Gefahr, dass Nutzer durch die suggerierte Einfachheit und Überschaubarkeit der Schutzziele dem Missverständnis unterliegen können, Datenschutzrecht-Compliance könne durch das „Abhaken" von wenigen Schutzzielen erreicht werden. Die eigentlichen Prüfkriterien, anhand derer die Gerichte und Aufsichtsbehörden die Rechtmäßigkeit von Datenverarbeitungen beurteilen, bleiben aber die rechtlichen Vorgaben der DSGVO und – soweit ergänzend anwendbar – des Bundesdatenschutzgesetzes (BDSG). Nach diesem Maßstab sind letztlich alle datenschutzrechtlichen Themen zu bewerten, und zwar unabhängig von einer Systematisierung von Schutzzielen.

Der dem Standard-Datenschutzmodell zugrundeliegende Gedanke, dass konkrete „best practise"-Hinweise das Datenschutzrecht nahbarer machen können, ist sicherlich richtig. Zur Erreichung dieses Ziels müssen diese konkreten Maßnahmenkataloge dann aber auch geliefert werden. Praktikable anwendbare Kataloge für alle denkbaren Konstellationen wird aber auch ein Anhang zum Standardmodell kaum liefern können.

Möglicherweise ist das Standard-Datenschutzmodell V2.0 nur der konzeptionelle Ausgangspunkt für eine Reihe von „best practise"-Referenzbausteinen, die zukünftig von den Aufsichtsbehörden erlassen werden. Diese Hoffnung bestand aber auch schon beim Erlass des Standard-Datenschutzmodells V1.0 im November 2016. Die für die praktische Anwendung des Standardmodells erforderliche Konkretisierung steht aber aktuell weiter aus, so dass die Überarbeitung des allgemeinen Teils durch die Aktualisierung auf V2.0 nur einen begrenzten Fortschritt darstellt.

Robert Bommel

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Robert Bommel, LL.M.
Wissenschaftlicher Mitarbeiter
T +49 521 96535 - 890
F +49 521 96535 - 114
M robert.bommel@brandi.net
www.brandi.net