Der Bayerische Landesbeauftragte
für den Datenschutz informiert
zum Thema

Datenschutzreform 2018

Die bereitgestellten Informationen sollen die bayerischen öffentlichen Stellen bei der Umstellung auf die Datenschutz-Grundverordnung unterstützen.
Sie wollen einen Beitrag zum Verständnis des neuen Rechts leisten, nehmen aber keine Verbindlichkeit in Anspruch.

München, 6. November 2017

Die Datenschutz-Grundverordnung (DSGVO): Anforderungen an Technik und Sicherheit der Verarbeitung

1. Einleitung

Bisher waren die rechtlichen Vorgaben zu den technischen und organisatorischen Maßnahmen, die für bayerische öffentliche Stellen relevant sind, grundlegend in Art. 7 Bayerisches Datenschutzgesetz (BayDSG) geregelt. Künftig finden sich die diesbezüglich maßgeblichen Regelungen vorwiegend in der Datenschutz-Grundverordnung.

Die Datenschutz-Grundverordnung trifft an mehreren Stellen Aussagen zu den technischen und organisatorischen Anforderungen an die Verarbeitung von personenbezogenen Daten:

- Art. 5 Abs. 1 Buchst. f DSGVO „Grundsätze für die Verarbeitung personenbezogener Daten“,
- Art. 24 DSGVO „Verantwortung des für die Verarbeitung Verantwortlichen“,
- Art. 25 DSGVO „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“,
- Art. 32 DSGVO „Sicherheit der Verarbeitung“,
- Art. 35 DSGVO „Datenschutz-Folgenabschätzung“,
- Art. 36 DSGVO „Vorherige Konsultation“.

2. Pflichten des Verantwortlichen

Wie schon in Teil 4 Nr. 1 des Überblicks zur Datenschutz-Grundverordnung dargestellt, richten sich die Regelungen der Datenschutz-Grundverordnung in erster Linie an den Verantwortlichen (siehe Art. 4 Nr. 7 DSGVO). Im vorliegenden Zusammenhang umfasst dies nach Art. 24 und Art. 32 DSGVO insbesondere die Pflicht, geeignete technische und organisatorische Maßnahmen einzusetzen, um zum einen sicherzustellen, dass eine Verarbeitung personenbezogener Daten mit den Vorgaben der Datenschutz-Grundverordnung in Einklang steht, und um zum anderen ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten.

Die Einhaltung dieser – und weiterer sich aus der Datenschutz-Grundverordnung ergebender – Pflichten ist durch den Verantwortlichen angemessen zu dokumentieren („Rechenschaftspflicht“, vgl. insbesondere Art. 5 Abs. 2, Art. 24 Abs. 1 Satz 1 DSGVO). Maßnahmen nach Art. 24 Abs. 1 Satz 1 DSGVO sind erforderlichenfalls zu überprüfen und zu aktualisieren (Art. 24 Abs. 1 Satz 2 DSGVO).

Hinweis: Gerade im Bereich der Dokumentation und Nachweisbarkeit steigen die Anforderungen durch die Datenschutz-Grundverordnung erheblich. Es sollte daher frühzeitig geprüft werden, welche Maßnahmen im Einzelnen ergriffen werden müssen (etwa Einhaltung von genehmigten Verhaltensregeln oder Zertifizierungsverfahren, vgl. Art. 24 Abs. 3 DSGVO). Es bietet sich an, ein übergreifendes Datenschutzmanagementsystem für alle Verfahren einzurichten.

Darüber hinaus erfordert die Überprüfungs- und Aktualisierungspflicht, auch bestehende Verfahren regelmäßig in Augenschein zu nehmen, insbesondere im Hinblick auf geänderte Rechtsvorschriften, auf wesentliche Verfahrensänderungen (etwa durch Hinzunahme neuer Datenarten), auf veränderte Zuständigkeiten sowie auch auf Weiterentwicklungen hinsichtlich des Standes der Technik (beispielsweise geänderte Anforderungen an Verschlüsselungsverfahren). Die insoweit durchgeführten Prüfungen müssen ebenfalls schriftlich dokumentiert werden.

3. Risikoanalyse

Die Datenschutz-Grundverordnung stellt die Rechte und Freiheiten der betroffenen Personen – also derjenigen, deren Daten verarbeitet werden – in den Vordergrund der (Sicherheits-)Betrachtungen. Art. 24 Abs. 1 Satz 1 und Art. 32 Abs. 1 DSGVO legen jeweils fest, dass die Erforderlichkeit von technischen und organisatorischen Maßnahmen unter Berücksichtigung „der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken (bzw. des Risikos) für die Rechte und Freiheiten natürlicher Personen“ geprüft werden muss.

Ähnlich wie im Bereich der IT-Sicherheit (siehe den „BSI-Grundschutz“) muss daher eine formale Risikoanalyse bei der Einführung eines neuen Verfahrens durchgeführt werden. Die Risikoanalyse ist zudem Grundlage für die Entscheidung, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO nötig ist. Kriterien für die Risikobewertung lassen sich vor allem den Erwägungsgründen 75 und 76, 89 bis 91 sowie 94 der Datenschutz-Grundverordnung entnehmen.

Im Rahmen der Risikoanalyse muss insbesondere abgewogen werden, in welchem Umfang und zu welchem Zweck personenbezogene Daten erhoben werden sollen, welchen Schutzbedarf die Daten haben und welche Gefahren/Risiken (genannt werden in Art. 32 Abs. 2 DSGVO insbesondere Risiken durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu personenbezogenen Daten) dies für die betroffenen Personen mit sich bringen kann. Dabei muss sowohl geprüft werden, wie schwerwiegend mögliche Nachteile für die betroffenen Personen sind, als auch, mit welcher Wahrscheinlichkeit diese eintreten können. Anschließend muss geprüft werden, mit welchen Maßnahmen das jeweilige Risiko reduziert werden kann. In diesem Zusammenhang nennt die Datenschutz-Grundverordnung ausdrücklich die Datenminimierung, die Pseudonymisierung sowie den Datenschutz durch Technikgestaltung (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default).

Die bayerischen öffentlichen Stellen sollten frühzeitig entscheiden, welche Methodik für die Risikoanalyse verwendet wird und durch welche Personen/Bereiche diese zukünftig durchgeführt werden soll.

4. Technische und organisatorische Maßnahmen, Datenschutz durch Technikgestaltung

Eine Auflistung von Datensicherheitsmaßnahmen, wie sie bisher in Art. 7 BayDSG enthalten war („Zehn Gebote“), sieht die Datenschutz-Grundverordnung nicht mehr vor. In Art. 25 und Art. 32 DSGVO werden jedoch einige Maßnahmen und Schutzziele in Bezug auf die Technik und Sicherheit der Datenverarbeitung aufgeführt. Diese beziehen sich teils unmittelbar auf die personenbezogenen Daten, teils aber auch auf die Systeme und Dienste, die im Zusammenhang mit der Datenverarbeitung eingesetzt werden (vgl. insbesondere Art. 32 Abs. 1 DSGVO).

Die Datenschutz-Grundverordnung (DSGVO):
Anforderungen an Technik und Sicherheit der Verarbeitung

Auch wenn hier teilweise neue Begrifflichkeiten und Systematiken verwendet werden, finden sich doch letztlich alle bisher schon aus dem Bayerischen Datenschutzgesetz abgeleiteten Sicherheitsanforderungen auch in der Datenschutz-Grundverordnung wieder:

- **Vertraulichkeit:** Schutz vor unbefugter Kenntnisnahme der Daten;
- **Integrität:** Gewährleistung der Echtheit, Vollständigkeit, Zurechenbarkeit, Urheberschaft und (Rechts-)Gültigkeit der Daten;
- **Verfügbarkeit:** zeitgerechte Bereitstellung von Daten, Möglichkeit zur ordnungsgemäßen Verarbeitung;
- **Belastbarkeit („Resilience"):** Dies ist ein neuer Begriff, der bisher im Datenschutzbereich nicht verwendet wurde. Im IT-Bereich ist mit „Resilience" üblicherweise eine gewisse Stabilität gegenüber Ausfällen oder Angriffen – wie etwa „Denial of Service"-Angriffen – gemeint. Die Abgrenzung zur Verfügbarkeit ist jedoch nicht eindeutig;
- **Wiederherstellbarkeit:** Dieser Begriff wurde bisher ebenfalls nicht als eigenständiges Schutzziel verwendet, da auch er dem Begriff der Verfügbarkeit zugeordnet werden könnte. Hierunter fallen Notfallkonzepte für Rechenzentren, um nach einem Ausfall oder Angriff schnell wieder betriebsbereit zu sein;
- **Data protection by design/Datenschutz durch Technikgestaltung:** Fragen des Datenschutzes müssen zukünftig bereits bei der Konzipierung von Verfahren und Produkten betrachtet werden. Dies betrifft etwa die Punkte Datenminimierung (Pflichtfelder), Pseudonymisierung, Möglichkeiten zur Datenlöschung, sichere Verschlüsselung und Berechtigungskonzept;
- **Data protection by default/datenschutzfreundliche Voreinstellungen:** Die Voreinstellungen von Produkten und Verfahren sollen so gestaltet sein, dass sie die Grundprinzipien des Datenschutzes und der IT-Sicherheit von vornherein berücksichtigen (Beispiele: keine Standard-Passwörter, Verschlüsselung aktiviert,

Beschränkung der Berechtigungen von Nutzenden, Ortungsdienste ausgeschaltet). Dieser Aspekt sollte zukünftig insbesondere bei der Beschaffung von Produkten berücksichtigt werden;

- **Pseudonymisierung, Verschlüsselung:** Diese beiden Maßnahmen dienen den Zielen der Vertraulichkeit und Integrität.

Bei der Auswahl der technischen und organisatorischen Maßnahmen ist gemäß Art. 25 DSGVO der „Stand der Technik“ zu beachten, der jedoch gesetzlich nicht näher definiert wird. Wie bisher auch, ist es daher sinnvoll, sich an öffentlich zugänglichen Standards zu orientieren, wie etwa an den Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik zu Schlüssellängen, Cipher-Suites oder zur WLAN-Konfiguration.

Für die Prüfung, ob eine konkrete technische und organisatorische Maßnahme erforderlich ist, müssen nach wie vor die Implementierungskosten mit den Ergebnissen der Risikoanalyse abgewogen werden. Zudem müssen der Schutzbedarf der Daten und die Ergebnisse der Risikoanalyse betrachtet werden. Je sensibler die Daten (siehe etwa besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO) und je höher die Risiken für die betroffenen Personen sind, desto umfassendere Maßnahmen sind erforderlich.

Hinweis: Die tatsächlich von bayerischen öffentlichen Stellen zu ergreifenden technischen und organisatorischen Maßnahmen zur Absicherung von Verfahren ändern sich durch die Datenschutz-Grundverordnung nicht zwangsläufig, auch wenn hier teilweise andere Begrifflichkeiten und Schutzziele verwendet werden. Allerdings steigt der Aufwand hinsichtlich der Vorabprüfung und Dokumentation von Maßnahmen in der Regel deutlich an. Es wird stets ein Datenschutzkonzept erforderlich sein, das die Risikoanalyse, die ergriffenen Maßnahmen und die regelmäßigen Prüfungen umfasst.

5. Handlungsempfehlungen

Nach allgemeiner Auffassung werden die Anforderungen der Datenschutz-Grundverordnung an Technik und Sicherheit nicht nur an neu zu entwickelnde Verarbeitungen, sondern auch an bereits bestehende Verarbeitungen zu stellen sein. Hinsichtlich des vorgeschriebenen Überprüfungsturnus wird derzeit voraussichtlich von einem Zwei- bis Drei-Jahres-Rhythmus ausgegangen.

Es wird daher empfohlen, frühzeitig mit der Überprüfung bestehender Verarbeitungen hinsichtlich ihrer Konformität mit den technischen und organisatorischen Vorgaben der Datenschutz-Grundverordnung zu beginnen, diese geeignet zu dokumentieren und ein Datenschutzmanagementsystem zu etablieren.

Bereits vor Inkrafttreten der Datenschutz-Grundverordnung sollten sich die bayerischen öffentlichen Stellen insbesondere einen Überblick darüber verschaffen, welche risikoverringernden Maßnahmen sie bereits getroffen haben und was noch zu tun ist, um auch den künftigen Vorgaben zu genügen.