Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 22.09.2020

Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen

Der Begriff „Digitale Souveränität“ wird in der öffentlichen Debatte in verschiedenen Bedeutungen verwendet. Nach der Definition des Kompetenzzentrums Öffentliche IT[1] ist in einem umfassenden Sinne Digitale Souveränität die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

Die Rolle der öffentlichen Verwaltung ist die gesetzesgebundene Erfüllung der Staatsaufgaben. Aus der Sicht der Verantwortlichen in der öffentlichen Verwaltung bedeutet Digitale Souveränität insbesondere, eigenständig entscheiden zu können, wie die in Art. 1 Datenschutz-Grundverordnung (DS-GVO) formulierten Ziele im Einklang mit den in Art. 5 DS-GVO festgelegten Grundsätzen für die Verarbeitung personenbezogener Daten, wie Rechtmäßigkeit, Transparenz, Zweckbindung und Sicherheit der Verarbeitung, umzusetzen sind. Dies erfordert nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) Wahlfreiheit und vollständige Kontrolle der Verantwortlichen über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten, gegebenenfalls unter Hinzuziehung des jeweiligen Auftragsverarbeiters.

Die Digitale Souveränität der öffentlichen Verwaltung ist jedoch nach einer für den Beauftragten der Bundesregierung für Informationstechnik durchgeführten „Strategischen Marktanalyse“[2] beeinträchtigt, „da die Geschäftsbeziehungen der öffentlichen Verwaltung mit externen, meist privaten IT-Anbietern erhebliche Abhängigkeiten verursachen. Danach resultieren diese Abhängigkeiten aus der technischen Beschaffenheit der IT-Landschaft, aus den stark auf Software ausgerichteten Prozessen, aus dem Umstand, dass sich die Beschäftigten an die eingesetzte Software gewöhnt haben, aus Vertragsklauseln sowie aus den bestehenden Marktgegebenheiten.“ Sie bringen Kontrollverlust und eine eingeschränkte Verfügbarkeit,

---

[1] Kompetenzzentrum Öffentliche IT (Hrsg.), Gabriele Goldacker, Digitale Souveränität, erhältlich unter https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t

[2] PwC Strategy& (Germany) GmbH, Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, erhältlich unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile

Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten mit sich. Auch vor diesem Hintergrund hat sich der IT-Planungsrat zum Ziel gesetzt, die digitale Souveränität der öffentlichen Verwaltung in ihren Rollen als Nutzer, Bereitsteller und Auftraggeber von digitalen Technologien kontinuierlich zu stärken.

Die Datenschutzkonferenz teilt die Einschätzung des IT-Planungsrats, dass die Digitale Souveränität der öffentlichen Verwaltung beeinträchtigt ist und sieht deren Gewährleistung als ein vordringliches Handlungsfeld an. Aus ihrer Sicht sind datenschutzrechtliche Vorgaben für große Softwareanbieter, die in der „Strategischen Marktanalyse“ empfohlene Diversifizierung durch den Einsatz alternativer Softwareprodukte sowie die Nutzung von Open Source Software besonders erfolgversprechende Handlungsoptionen. Durch den Einsatz von Open Source Software kann die Unabhängigkeit der öffentlichen Verwaltung von marktbeherrschenden Softwareanbietern dauerhaft sichergestellt werden. Konkret fordert die Datenschutzkonferenz Bund, Länder und Kommunen dazu auf, langfristig nur solche Hard- und Software einzusetzen,

- die den Verantwortlichen die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik belässt, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Zustimmung der Verantwortlichen im Einzelfall erfolgen,

- bei der alle zur Verfügung stehenden Sicherheitsfunktionen für Verantwortliche transparent sind und

- die eine Nutzung der Hard- und Software sowie den Zugriff auf personenbezogene Daten ermöglicht, ohne dass Unbefugte davon Kenntnis erhalten und ohne dass unzulässige Nutzungsprofile angelegt werden können.

Kurzfristig erfordert die Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in Bund, Ländern und Kommunen zur Einhaltung der datenschutzrechtlichen Anforderungen insbesondere:

1. Verbesserte Möglichkeiten der datenschutzrechtlichen Beurteilung von Produkten und Dienstleistungen – sowohl bei der Auswahl als auch im laufenden Betrieb:

    - Zertifizierungen können Verantwortlichen die Prüfung und Kontrolle erleichtern, wenn sie sich nicht eigenständig ein valides Bild über die komplexe Funktionsweise von Informationstechnik machen können.

    - Die Ministerialebene sollte in die Pflicht genommen werden, Vorgaben für die öffentliche Verwaltung zu machen.

    - Zudem sollten Behörden stärker kooperieren, um die erforderliche Expertise selbst bereitstellen zu können.

2. Berücksichtigung der Ziele und Kriterien der Digitalen Souveränität bei der Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen:

- Für die Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen sollten im Einklang mit dem europäischen Vergaberecht Ausschreibungskriterien entwickelt werden, um bei der Vergabe solche Anbieter bevorzugt auswählen zu können, welche Digitale Souveränität ermöglichen.

3. Nutzung von offenen Standards durch die Produktentwickler, damit die Verantwortlichen auch tatsächlich in die Lage versetzt werden, Anbieter und Produkte zu wechseln, wenn sie mit deren Produkten und Dienstleistungen die Datenschutzanforderungen nicht (mehr) oder nur ungenügend umsetzen können:

    - Die Nutzung von offenen Standards kann durch deren inhärente Transparenz dazu beitragen, die Überprüfbarkeit zu sichern und eine Kontrolle zu erleichtern. Dies betrifft Systemsoftware und insbesondere Datenformate, aber auch Datenbanken und Anwendungssoftware, die auf Software-Plattformen aufsetzen. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden. Insbesondere können hierbei über die Einrichtung von Bund-/Länder-/Kommunen-übergreifenden Entwicklungsverbünden Aufwände verteilt und Skaleneffekte gehoben werden. Daher sollten Verantwortliche den Einsatz von Produkten und Dienstleistungen bevorzugen, die offene Standards verwenden.

4. Veröffentlichung des Quellcodes und der Spezifikationen öffentlich finanzierter digitaler Entwicklungen:

    - Wenn Software oder Hardwarestandards unter finanzieller Beteiligung der öffentlichen Hand entwickelt werden, sollten diese standardmäßig so veröffentlicht werden, dass diese nachvollzogen werden können.

    - Standardmäßig sollten diese so ausgestaltet werden, dass eine öffentliche Weiterentwicklung möglich ist (Open Source Lizenzen).

5. Möglichkeiten zur Steuerung des Zugriffs auf Daten, der Konfiguration von Systemen und der Gestaltung von Prozessen:

    - Verantwortliche müssen über tatsächliche Steuerungsmöglichkeiten verfügen, insbesondere, um ihre Pflichten nach Art. 25 DS-GVO erfüllen zu können. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Verantwortliche sollten nur solche Produkte und Dienstleistungen beschaffen und nutzen, die diese Prinzipien beachten. Organisationen mit verteilter Verantwortung (etwa Kommunen, Bundesländer oder auch beteiligte Dienstleister wie Konzerne) müssen auch bei zentral beschafften oder betriebenen Komponenten wie Hardware, Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten. Bei zentral bereitgestellten Anwendungen, etwa in einer derzeit im IT-Planungsrat diskutierten „Verwaltungscloud“, ist es eine notwendige Voraussetzung,

dass die jeweiligen datenschutzrechtlichen Vorgaben der Verantwortlichen für Betrieb und Konfiguration individuell umgesetzt werden können. Das ist bei der Konzeption zu berücksichtigen.

Die Datenschutzkonferenz ist der Ansicht, dass die Stärkung der Digitalen Souveränität große strategische Bedeutung für die öffentliche Verwaltung hat und gemeinsam und kontinuierlich vorangetrieben werden muss. Sie fordert Bund, Länder und Kommunen dazu auf, die in der Entschließung aufgeführten Kriterien für eine Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in den Bereichen IT-Beschaffung sowie System- und Fachverfahrensentwicklung zu berücksichtigen.