Datenpolitik für Alle: Regelungen gegenüber der öffentlichen Hand

Der SPD-Parteivorstand, die SPD-Bundestagsfraktion, sowie die SPD-Landtagsfraktionen werden aufgefordert, die Verfügbarkeit von Daten seitens der öffentlichen Hand zu fördern, wobei eine gute Datenpolitik organisatorische und technische Vorkehrungen für einen wirksamen Datenschutz treffen muss.

Präambel (und zugleich Begründung):

Spätestens mit der Verbreitung des Internets hat sich unser Zusammenleben immer stärker zu einer Informations- und Wissensgesellschaft gewandelt, in der Informationen und das Wissen nebst kulturellen Bereicherungen eine immer größere Bedeutung gewinnen. Für Deutschland als das Land der Dichter und Denker sollte dies ein Heimspiel und eine Herausforderung zugleich sein.

Wissen ist Macht. In einer Demokratie, bei der die Macht dem Volke zusteht, folgt daraus, Wissen und Informationen möglichst breit, vielfältig und leicht allen Bürgerinnen und Bürgern aber auch den Unternehmen zugänglich zu machen. Freilich gilt dies nur soweit, wie der Datenschutz, der Schutz der Privatsphäre und andere Geheimnisbereiche (z.B. Betriebsgeheimnisse, Dienstgeheimnisse) dem nicht entgegenstehen. Vornehmlich sollen demnach bereits rechtmäßig veröffentlichte Informationen und Daten aus Verwaltungsvorgängen, für die es kein überwiegendes Geheimhaltungsbedürfnis gibt, den Bürgerinnen und Bürgern möglichst barrierefrei zugänglich sein. Weiterhin ist darauf zu achten, kulturelle und wissenschaftliche Daten möglichst breit zur Verfügung zu stellen, um die gesellschaftliche Teilhabe und eine Chancengleichheit für alle zu fördern. Daten für alle heißt auch Kultur und Wissen für alle.

Unseren Grundrechten liegt das Prinzip der Selbstbestimmung zugrunde und zwar insbesondere in Form der informationellen Selbstbestimmung. Daraus folgt die Macht über die Verwendung und Verbreitung der einen selbst betreffenden personenbezogenen Daten zuverlässig und wirksam grundsätzlich bei der Person selbst zu verorten. Datenpolitik muss deshalb die digitale Welt in Einklang mit unseren Grundwerten ordnen und organisatorische und technische Vorkehrungen für

einen wirksamen Datenschutz und eine angemessene Wahrung der Privatsphäre treffen.

Die Europäische Union hat unter dem Stichwort „Ein Europa für das digitale Zeitalter“ den Entwurf für ein Data Governance Act[1] vorgelegt und strebt eine Erhöhung der Verfügbarkeit von Daten und die Ausschöpfung deren wirtschaftlichen und gesellschaftlichen Potenzials an.

Beschlusstext:

Aus diesen Erwägungen ergeben sich gegenüber der öffentlichen Hand die nachfolgenden Regelungen die der SPD-Bundestagsfraktion sowie der SPD-Landtagsfraktion zur Umsetzung empfohlen werden:

1. Informationsfreiheitsgesetze

Informationsfreiheitsgesetze, die jedem einen Anspruch auf Auskunft über Daten aus der öffentlichen Verwaltung verschaffen, müssen auf allen Verwaltungsebenen (nicht nur in Bund und Ländern) wirken und zwar unter Einschluss der Sondervermögen der öffentlichen Hand und der von ihr beherrschten Tochterunternehmen. Entsprechend dem Vorbild in den bereits existierenden Informationsfreiheitsgesetzen sorgt dann ein Informationsfreiheitsbeauftragter für eine möglichst reibungsfreie Durchführung dieses Anspruchs und unterstützt sowohl Bürgerinnen und Bürger als auch die öffentliche Hand und ihre Tochterunternehmen bei der Anwendung dieser Gesetze.

2. Daten für alle:

In der öffentlichen Hand befindliche Daten, die zweifelsfrei keinen Personenbezug aufweisen und deren Veröffentlichung keine wesentlichen Sicherheitsinteressen, Geheimhaltungs- oder Vertraulichkeitspflichten entgegenstehen,[2] sind digital in strukturierten Formaten, kosten- und barrierefrei und gut auswertbar über das Internet zur Verfügung zu stellen. Hierzu zählen nicht nur sämtliche Rechtsnormen[3] und öffentliche Allgemeinverfügungen[4] sondern auch technische Normen[5], meteorologische Daten, Mobilitätsdaten[6], Energiedaten[7] sowie Daten aus Landwirtschaft[8] und aus der Industrie[9]. Dabei sollte Deutschland schon jetzt über den bereits in der EU-Richtlinie über offene Daten und die Weiterverwendung von

Informationen des öffentlichen Sektors (2019/1024) enthaltenen Katalog von per API-Schnittstelle verfügbaren, hochwertigen Datensätzen hinausgehen und möglichst umfassend die keinen Personenbezug aufweisenden Datensätze für entsprechende Schnittstellen definieren.

Darüber hinaus soll geprüft werden, ob auch gesellschaftlich relevante Daten wie Registerdaten (z.B. Unternehmensregister, Handelsregister, Vereinsregister) und Katasterdaten (Größe, Lage und Eigentümerschaft von Grundstücken) ebenso frei über das Internet zugänglich gemacht werden können, auch wenn diese Daten in gewissem Umfang personenbezogene Informationen (Name und Anschrift) aufweisen. Die Kundgabe von Namen und Kontaktadressen von natürlichen Personen sollen jedoch ungeprüft nur als Initialen und auf gesonderte und pseudonymisierte e Mailadressen beschränkt sein.

3. Datentreuhänder:

Weiterhin sollen öffentlich-rechtlich basierte, vom Bundesdatenschutzbeauftragten zertifizierte und kontrollierte Datentreuhänder dafür dienen, aus Datensammlungen mit personenbezogenen Daten, den Anteil nicht personenbezogener Daten zuverlässig zu extrahieren und soweit möglich die personenbezogenen Daten zu anonymisieren, um einen solchen Datenbestand ebenfalls öffentlich zur Verfügung zu stellen.

Solche Datentreuhänder sollen auch helfen, Zweifelsfälle zu klären und im Falle einer Weigerung der öffentlichen Stelle zur Datenfreigabe hierzu eine Stellungnahme abgeben. Für solche Zweifels- und Konfliktfälle ist eine Verwaltungspraxis zu etablieren, die die Datenschutznotwendigkeit sorgfältig prüft und bei negativem Ausgang dieser Prüfung als Standard[10] zu einem offenen Zugang der Daten führt (Open-Data).

4. Dezentralisierung der Datenbestände, keine Datensilos:

Zur Sicherstellung der vorgenannten Ziele bedarf es einer starken personellen Aufwertung der Datenschutzbehörden in Bund und Ländern sowie in Europa. Insbesondere gegenüber den großen Datensammlern wie Google, Apple, Facebook, Amazon und Microsoft bedarf es eines konzertierten und wirksamen Auftretens seitens der Datenschützer in Europa.

Hinsichtlich solcher und anderer Datensilos sind das Prinzip der Dezentralisierung zu verfolgen und Strukturen anzustreben, mit denen die Daten möglichst nicht in den Datensilos der Unternehmen, sondern allein in den Endgeräten der Nutzer gespeichert werden.

Ergänzende Hinweise zum Text:

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

[2] Zum Beispiel bei Dienst-, Betriebs- und Geschäftsgeheimnissen

[3] Mithin nicht nur Gesetze und Verordnungen sondern auch Bebauungspläne und Satzungen

[4] z.B. Verkehrszeichen

[5] z.B. DIN-Normen

[6] z.B. Regensensoren an Ampeln, Fahrzeugmaße, anonyme Verkehrsdaten

[7] z.B. Echtzeitmessung der Stromeinspeisung

[8] z.B. Stromverbrauch von Maschinen

[9] z.B. Informationen über Produkte; nicht über die Produktion oder über Geschäfte

[10] Entsprechend der Maxime in Art. 5 Abs. 2 der EU-Richtlinie 2019/1024