Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Grundsatzpositionen und Forderungen für die neue Legislaturperiode

Die fortschreitende Digitalisierung eröffnet wirtschaftliche und gesellschaftspolitische Chancen. Mit ihr einher gehen jedoch erhebliche Risiken für die Persönlichkeitsrechte der Menschen. Ein an diese Entwicklungen angepasster und damit starker Datenschutz ist das Gebot der Stunde.

Die Datenschutzkonferenz formuliert zu Beginn der Legislatur elf handlungsorientierte Grundforderungen, deren Ziel es ist, das Datenschutzrecht weiter zu entwickeln und seine Durchsetzung und Akzeptanz zu fördern. Ein wirksamer Datenschutz ist Grundrechtsschutz und darf nicht als Hindernis betrachtet werden. Er muss vielmehr als integraler und förderlicher Bestandteil politischer, wirtschaftlicher und gesellschaftlicher Fortentwicklung verstanden und gelebt werden.

Digitale Souveränität – Datensouveränität

Die DSK fordert, das Verbotsprinzip nach der DSGVO nicht durch den Anspruch auf „Datensouveränität" aufzuweichen.

„Datensouveränität" ist ein Schlagwort in der politischen Auseinandersetzung um die zeitgemäße Positionierung des Datenschutzes, das in unterschiedlichen Zusammenhängen gebraucht wird. Aus der Alltagssprache entnommen, wird der aus dem Staatsrecht stammende Begriff „Souveränität" mit selbstbestimmtem Handeln assoziiert, der einen Anspruch auf (absolute) Herrschaft über die eigenen persönlichen Daten beinhaltet. Dies allerdings kommt nach gegenwärtigem Rechtsverständnis allenfalls im Kernbereich privater Lebensgestaltung in Betracht. Zudem trifft er datenschutzrechtliche Anforderungen ebenso wenig wie das mit dem neuen Begriff angestrebte Ziel, Daten zu einer rein wirtschaftlichen Größe zu machen und damit Einschränkungen des Datenschutzes zu verschleiern. Die DSK spricht sich daher dafür aus, auch künftig das aus der Menschenwürde abgeleitete Recht auf informationelle Selbstbestimmung in den Mittelpunkt zu stellen und bei dem funktionalen Begriff des datenschutzrechtlichen Verbotsprinzips zu bleiben.

Grundsatz der Datenminimierung

Die DSK fordert, der Datenminimierung die ihr gemäß DSGVO gebührende Überholspur auf dem Weg der Digitalisierung frei zu räumen.

Datenminimierung heißt, dass personenbezogene Daten auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein müssen. Dies ist notwendig, um die mit der Datenverarbeitung einhergehenden Risiken für die betroffenen Personen einzudämmen. Der Grundsatz der Datenminimierung lässt sich aus dem Verfassungsrecht der EU und Deutschlands ableiten und wurde zu einem der Hauptprinzipien der DSGVO erhoben (Art. 5 Abs. 1 lit. c DSGVO). Damit ist Datenminimierung Rahmenbedingung jeder Datenverarbeitung in Europa und steht nicht zur Disposition des deutschen Gesetzgebers.

Hierdurch werden Innovationen nicht verhindert: Clevere Datenminimierungslösungen können das Bedürfnis zur Auswertung von Informationen und die Notwendigkeit des Datenschutzes vereinen, z. B. indem auf den Personenbezug von Daten verzichtet wird. Technologische Projekte, die Datenminimierung innovativ und intelligent umsetzen und damit erst rechtskonforme Geschäftsmodelle im Zusammenhang mit Big Data-Anwendungen und „smarten“ Lösungen ermöglichen, sollten gefördert werden.

Rahmenbedingungen für datenschutzfreundliche und sichere Systemgestaltung

Die DSK fordert, datenschutzfreundliche und sichere Systemgestaltung stärker öffentlich zu fördern.

Nach der DSGVO sollen nicht nur die erforderlichen technisch-organisatorischen Maßnahmen für Datensicherheit getroffen werden, sondern Datenschutz soll von Anfang an und über den gesamten Lebenszyklus hinweg in Produkte, Dienste und Anwendungen eingebaut sein.

Daher sollten Initiativen und Projekte verstärkt gefördert werden, die Datenschutz „by Design“ und „by Default“ gewährleisten und die Qualität der Datensicherheit verbessern. Die DSK fordert die Bundesregierung auf, sich für technologische Innovationen mit eingebautem Datenschutz einzusetzen und diese auch im Austausch mit Vertretern aus Wirtschaft, Forschung und Entwicklung voranzubringen. Auch sollten alle von der Bundesregierung geförderten Vorhaben mit Personenbezug zukünftig belegen, wie sie die Datenschutzanforderungen erfüllen, damit die Resultate rechtskonform sind. Datenschutzfreundliche und sichere Systemgestaltung ist im Sinne der Vorbildfunktion des öffentlichen Sektors in den öffentlichen Stellen des Bundes sowie in bestehenden oder aufzubauenden IT-Infrastrukturen nachzuweisen. Im Bereich der nationalen, europäischen und internationalen Standardisierung soll die Bundesregierung darauf hinwirken, dass Datenschutzanforderungen eine entsprechende Berücksichtigung finden. Dies betrifft auch einheitliche Vorgaben und Schnittstellen für den Selbstdatenschutz und ein angemessenes Niveau bei Zertifizierungen.

Klare gesetzliche Regelungen für automatisierte Entscheidungen durch Algorithmen

Die DSK fordert, für den Einsatz von Algorithmen im Hinblick auf Transparenz, Kontrolle und Begrenzung klare gesetzliche Regelungen zu schaffen.

Die digitale Informationsgesellschaft ist von Verfahren geprägt, die in unterschiedlichster Art und Weise automatisierte Entscheidungen treffen. Hinter ihnen verbergen sich Algorithmen, bei denen oft nicht ersichtlich ist, welche Daten als Grundlage für Entscheidungen herangezogen werden bzw. wie diese der Entscheidungsfindung dienen. Die Komplexität von Algorithmen macht es häufig unmöglich, ihre Funktionsweise analytisch zu bewerten. Sie entscheiden bspw. über Fahrzeugreaktionen, ob ein Kredit gewährt oder welcher Versicherungstarif angeboten wird und das meist ohne Berücksichtigung der individuellen Situation betroffener Personen. Es besteht die Gefahr von Diskriminierungen und Stigmatisierungen, eingeschränkten Auswahlmöglichkeiten bis hin zu Fehlentscheidungen. Menschen dürfen algorithmischen Entscheidungen nicht bedingungslos ausgeliefert werden. Es bedarf daher Regelungen zu Einsatzvoraussetzungen, Entwicklung, Prüfung und Verwendung von Algorithmen, deren Einsatzzweck in automatisierten Entscheidungen liegt.

Nachbesserungen beim BDSG

Die DSK fordert, die Einschränkung von Aufsichtsbefugnissen und Betroffenenrechten zurückzunehmen sowie die Regelungen zur Videoüberwachung europarechtskonform auszugestalten.

Den Untersuchungsbefugnissen der Aufsichtsbehörden sind Datenverarbeitungen entzogen, die dem Steuergeheimnis, der ärztlichen Schweigepflicht oder anderen Geheimhaltungspflichten unterliegen. Diese Beschneidung der Befugnisse gegenüber Berufsgeheimnisträgern geht weit über die Öffnungsklausel des Art. 90 DSGVO hinaus. Es sollte die bisherige Regelung des § 38 Abs. 3, 4 i. V. m. § 24 Abs. 2 und Abs. 6 BDSG-alt beibehalten werden. Die Aufsicht durch unabhängige Datenschutzbehörden dient den Interessen der betroffenen Personen. Geheimhaltungspflichten sind durch § 29 Abs. 3 S. 2 BDSG hinreichend geschützt.

Übermäßige Einschnitte in die Betroffenenrechte widersprechen dem Schutzcharakter der DSGVO. Beschränkungen dürfen nicht den Wesensgehalt der Grundrechte und Grundfreiheiten tangieren, müssen in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahmen darstellen sowie die in Art. 23 Abs. 1 DSGVO aufgezählten Ziele sicherstellen.

Die Vorschrift zur Videoüberwachung ist, soweit sie nicht-öffentliche Stellen betrifft, zu streichen. Sie lässt sich nicht auf den herangezogenen Art. 6 Abs. 1 S. 1 lit. e) i.V.m. Art. 6 Abs. 3 S. 1 DSGVO stützen. Zudem erlaubt die ohnehin unmittelbar geltende DSGVO einen angemessenen Ausgleich zwischen den berechtigten Interessen der Verantwortlichen an einer Videoüberwachung und dem Schutz der Persönlichkeitsrechte der Betroffenen.

Innere Sicherheit unter Wahrung des Datenschutzes

Die DSK fordert, bei der Bekämpfung von Terrorismus und Kriminalität das Vertrauen unbescholtener Menschen in die Vertraulichkeit ihrer Kommunikation und die Unberührtheit ihrer Privatheit zu wahren.

Datenschutz steht nicht im Widerspruch zu Sicherheit. Datenschutz schafft Sicherheit, denn das Grundrecht auf Schutz personenbezogener Daten verlangt klare gesetzliche Regelungen, die transparent für den Einzelnen die Leitplanken für die Ausübung seiner Rechte und deren Grenzen festlegen. Datenschutz bringt Rechtsklarheit und Rechtsklarheit trägt zur Steigerung des Gefühls der Sicherheit bei. Nur Sicherheit in Freiheit ist wirkliche Sicherheit für alle.

Auch das Verhalten im öffentlichen Raum muss grundsätzlich von Beobachtung, Aufzeichnung, biometrischer Erfassung und automatisierter Auswertung frei bleiben. Eine massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht den Grundrechten. Die Vorratsdatenspeicherung ist daher in all ihren Ausprägungen auf den Prüfstand zu stellen. Befugnisse zu Überwachungsmaßnahmen müssen einem gestuften System folgen, wonach sich die Rechtfertigung für einen Grundrechtseingriff an der Eingriffsintensität bemisst.

Betroffene sind über sicherheitsbehördliche Maßnahmen zu informieren. Sollte dies nicht möglich sein, ist umso mehr eine unabhängige Kontrolle zu gewährleisten: Eine effektive Datenschutzkontrolle muss Sanktions- und Anordnungsbefugnisse und auch die Kontrolle der Nachrichtendienste umfassen. Auch grenzüberschreitende Datenübermittlungen dürfen davon nicht ausgeschlossen sein. Diese Prinzipien sind bei einer Änderung oder Neufassung von Sicherheitsgesetzen auch aus Anlass der Anpassung an Vorgaben der EU zu beachten.

Arbeiten 4.0 – ein Beschäftigtendatenschutzgesetz für die neue Arbeitswelt

Die DSK fordert, den Beschäftigtendatenschutz durch ein eigenständiges Gesetz zu regeln

§ 26 BDSG-neu übernimmt weitgehend die bisher geltenden Regelungen des BDSG-alt. Diese sind jedoch unzureichend. Die Arbeitswelt 4.0 erweitert z. B. die Möglichkeiten der offenen und verdeckten technischen Überwachung erheblich. Ein angemessener Ausgleich zwischen Informationsinteressen des Arbeitgebers und Schutz der Rechte und Freiheiten des Arbeitnehmers ist nur durch eine differenzierte, umfassende gesetzliche Regelung zu erreichen.

Big Data im Gesundheitswesen

Die DSK fordert, für die Auswertung von Gesundheitsdaten strikte gesetzliche Vorgaben zu machen.

Gesundheitsdaten unterliegen dem strengeren Regelungsregime für besondere Kategorien personenbezogener Daten. Zunehmend werden sehr große Mengen von Gesundheitsdaten aus den unterschiedlichsten Lebensbereichen zusammengeführt und mit sog. Big Data-Anwendungen systematisch ausgewertet.

Verknüpfungen zwischen verschiedenen Datenbeständen, die Gesundheitsdaten enthalten, dürfen nur auf der Grundlage spezieller rechtlicher Regelungen zugelassen werden. Die Re-Identifizierung und unerlaubte Zusammenführung von Daten, das Anlegen von Datenprofilen zu einer Person sowie der Handel mit Gesundheitsdaten sind zu verbieten und unter Strafe zu stellen. Es muss zudem gesetzlich festgelegt werden, dass mit anonymisierten bzw. hinreichend pseudonymisierten Daten gearbeitet wird, in welchen Zusammenhängen ausnahmsweise auf die Einwilligung als Legitimation für eine Verarbeitung von Gesundheitsdaten in Big Data-Anwendungen zurückgegriffen werden darf und unter welchen Voraussetzungen eine wirksame Einwilligung gegeben werden kann. Zudem sind Transparenzvorgaben z. B. hinsichtlich der Analysemethoden, der Verarbeitungszwecke und der genutzten Datenbestände bei geplanten Big Data-Projekten zu machen. Es sollte gesetzlich vorgesehen werden, dass für jedes Big Data-Projekt im Gesundheitswesen das Votum der zuständigen Datenschutzaufsichtsbehörde eingeholt wird.

E-Health

Die DSK fordert, bei der Digitalisierung des Gesundheitswesens („E-Health“) das Recht auf Schutz personenbezogener Daten der Patienten und Versicherten gesetzlich wirksam zu sichern.

Auch künftig muss das Vertrauensverhältnis zwischen Patienten und ihren Behandlern effektiv geschützt werden. Vor einer Nutzung neuer technischer Anwendungen ist deshalb ein den Anforderungen der DSGVO genügender Datenschutz- und Datensicherheitsstandard sicherzustellen. Bei einer Integration mobiler oder anderer neuer Technologien in die Regelversorgung sowie in das E-Health-System ist deren datenschutz- und datensicherheitsgerechte Ausgestaltung zu garantieren. Ebenso ist Transparenz für die Nutzer herzustellen.

Zu verhindern ist, dass Gesundheitsdaten zur Bemessung von Versicherungstarifen laufend erhoben und vertragsbegleitend genutzt werden. Im Bereich der Krankenversicherung drohen mit der Erhebung von Gesundheitsdaten mittels sog. Wearables und Fitness-Apps Diskriminierungen von Versicherten durch das Angebot gesundheitsbezogener Tarife. Bei der Bemessung von Versicherungstarifen dürfen nicht die Patienten und Versicherten benachteiligt werden, die einer umfassenden Erfassung und Übertragung von Gesundheitsdaten nicht zustimmen.

Mit Datenschutz E-Government gestalten

Die DSK fordert, für die verwaltungsebenenübergreifende Umsetzung von E-Government Verwaltungsdienstleistungen sicher und datenschutzgerecht anzubieten.

Das Onlinezugangsgesetz schafft zwar durch einen Portalverbund zwischen allen Verwaltungsangeboten des Bundes, der Länder und der Kommunen sowie ein Nutzerkonto für jedermann die rechtlichen Voraussetzungen. Die DSK weist aber darauf hin, dass E-Government Akzeptanz in der Verwaltung wie bei den Bürgern bedingt.

Die DSK fordert deshalb Bund und Länder auf, mit Datenschutz E-Government konsequent vertrauenswürdig zu gestalten, im Sinne eines Datenschutzes „by Design“ und „by Default“. Die Ende-zu-Ende-Verschlüsselung der Kommunikation, Konzepte mit Datenschutzgarantien (z. B. datenschutzkonforme Bezahlsysteme und deutsche oder europäische „Trusted-Cloud“-Lösungen) und ein umfassendes Datenschutz- und Informationssicherheitsmanagement bilden dafür wesentliche Grundlagen. Rechtskonform müssen auch neue Entwicklungen wie „Data Driven Government“ – Verwaltungsentscheidungen auf Basis von Daten und Analysen – umgesetzt werden: mit Techniken zur Anonymisierung und Aggregation statt zentralisierter Anhäufung und Auswertung personenbezogener Daten.

Stärkung des internationalen Datenschutzes

Die DSK fordert die Bundesregierung auf, sich bei Entscheidungen der Europäischen Kommission über die Zulässigkeit von Datentransfers in Drittstaaten für ein hohes Datenschutzniveau einzusetzen. Zudem sind Versuche abzuwehren, den Datenschutz durch internationale Handelsverträge einzuschränken.

Das Bestreben der Europäischen Kommission, Drittstaatentransfer auf der Basis von Angemessenheitsbeschlüssen zu vereinfachen, darf nicht zu einer Erosion des Grundrechts auf informationelle Selbstbestimmung führen.

Die Bundesregierung sollte sich daher dafür einsetzen, dass die vom EuGH (C-362/14) aufgestellten Grundsätze Maßstab für Angemessenheitsentscheidungen bleiben. Künftige Handelsverträge dürfen den Datenschutz nicht aushöhlen, indem datenschutzrechtliche Regelungen als Handelshemmnis angesehen oder zum Gegenstand etwaiger Investor-Staat-Streitverfahren werden. Auch datenschutzrechtliche Standards im Europarat, in der OECD und den Vereinten Nationen müssen ein vergleichbar hohes Datenschutzniveau aufweisen.