Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Datenschutzpolitische Agenda für die 20. Wahlperiode des Deutschen Bundestages

Vorschläge des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die Wahlprogramme und Koalitionsvereinbarungen der Parteien

Bonn im Dezember 2020

Datenschutz ist Grundbedingung einer freien rechtstaatlich orientierten Gesellschaft. Gleichzeitig ist Datenschutz Motor der Digitalisierung, wenn Menschen dem Schutz ihrer Privatsphäre vertrauen und dadurch Veränderungen annehmen können. Die kommende 20. Wahlperiode des Deutschen Bundestages ist entscheidend für die weitere Zukunft unseres digitalen Zusammenlebens und den Digitalstandort Deutschland. Der digitale Wandel hat alle Lebensbereiche erfasst. Deshalb ist es unerlässlich, Fragen der Freiheit und Selbstbestimmung im digitalen Zeitalter den notwendigen Raum bei politischen Projekten zu geben. Vor diesem Hintergrund empfiehlt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im Rahmen seines gesetzlichen Auftrags zur Beratung den Parteien, folgende Themen für die nächste Legislaturperiode in den Blick zu nehmen:

I. Digitales Leben, Wirtschaften und Arbeiten

- Umfassender Datenschutz für Kinder und Jugendliche

  Für Kinder und Jugendliche gehört die Nutzung digitaler Medien wie selbstverständlich zum Alltag. Die Folgen der Datenverarbeitungen und hierdurch entstehenden Risiken können sie allerdings noch schwerer als Erwachsene abschätzen. Nur durch eine möglichst früh ansetzende Förderung ihrer Medien- und Datenschutzkompetenz gelingt es, ein Bewusstsein für Gefahren zu wecken. Hierzu müssen dringend verstärkte Anstrengungen unternommen werden, wie etwa eine bundesweite Aufklärungskampagne unter Einbeziehung der Eltern als Bestandteil des schulischen Bildungsangebots. Zudem sollte der DigitalPakt Schule des Bundes datenschutzfreundliche Hard- und Software Lösungen in Schulen sowie Kinder- und Jugendzimmern forcieren, besonders wenn es um Homeschooling und Hybridunterricht in Zeiten der Pandemie geht. Für Kinder bis zu einem gewissen Alter sollte überdies die Verarbeitung ihrer Daten durch Internetdienste zu Werbezwecken oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen („Kinder-Profiling“) durch eine Initiative auf EU-Ebene ausdrücklich verboten werden.

- Recht auf anonymes digitales Bezahlen schaffen

  Die mit der Ausweitung des digitalen Zahlungsverkehrs verbundenen wirtschaftlichen und staatlichen Interessen gefährden die für Klein- und Kleinsttransaktionen verbliebene Privatheit des geschäftlichen Alltags. Nur der klassische Bargeldverkehr schützt bisher vor der vollständigen digitalen Erfassung und Dokumentation jeglicher Alltagsgeschäfte durch private Unternehmen. Nicht zuletzt deshalb ist er in der Bevölkerung breit akzeptiert und vielfach weiter gewünscht; er sollte erhalten bleiben. Gerade die aktuelle Pandemie zeigt aber auch die Nachteile des Bargeldverkehrs beziehungsweise die Vorzüge des bargeldlosen Bezahlens. Um auch in diesem Bereich die Akzeptanz der Bevölkerung zu erhöhen und die Digitalisierung ohne Verlust von Privatheit zu ermöglichen, muss es auch in der digitalen Welt einen Rechtsanspruch auf anonymes bargeldloses Bezahlen bei kleineren Geldbeträgen geben. Dies steht dann auch nicht im Widerspruch zur Bekämpfung illegaler Transaktionen und Geldwäscheprävention.

- Datenschutz und Datensicherheit im Produktsicherheitsrecht verankern

  Für Smartphones, Tablets, Wearables und andere Smart Devices, aber auch für eine Vielzahl von Sensoren, etwa im Smart Home oder in automatisiert fahrenden Fahrzeugen gilt: sie alle können uns umfangreich ausforschen. Bisher müssen Hersteller allerdings nicht unmittelbar für die Sicherheit und Datenschutzkonformität ihrer Produkte einstehen, solange sie nicht als datenschutzrechtlich verantwortliche Stelle agieren. Deshalb muss durch einen spezifischen Rechtsrahmen auf EU-Ebene sichergestellt sein, dass die Grundsätze von Privacy by Design und Default schon in die Produktentwicklung einfließen und bereits „ab Werk“ umfassend umgesetzt werden. Es sollte dabei gesetzlich geregelt werden, dass jede Datenverarbeitung nach Möglichkeit ausschließlich zweckbestimmt in einem geschlossenen System vorzugsweise dezentral erfolgt, dabei anfallende Daten vor jedem unautorisierten Zugriff geschützt sind und eine Übermittlung an Dritte ohne Zutun betroffener Personen ausgeschlossen werden kann.

- Datenschutz in intelligenten Verkehrssystemen regeln

  Die Mobilität der Zukunft braucht klare Regeln – auch im Bereich des Datenschutzes. Nirgendwo sonst sind so umfassendere Datenflüsse und Profile möglich. Nur frühestmögliche Anonymisierungen sowie strikte Zweckbindungen und Zweckänderungsverbote stellen sicher, dass dort, wo Daten fließen, die informationelle Selbstbestimmung nicht auf der Strecke bleibt. Deutschland als erfolgreicher Entwicklungsstandort verschiedener Verkehrsträger sollte auch beim Privacy by De-

sign im Smart Mobility führend werden – technisch und den Rechtsrahmen betreffend. Beispielsweise ist es notwendig, dass fahrzeugtechnische Vorschriften nicht nur die Verkehrssicherheit und Umweltverträglichkeit, sondern auch einen ausreichenden Schutz der Privatsphäre gewährleisten. Im Straßenverkehrsgesetz sollte für die Car-to-Car-Kommunikation geregelt werden, dass zwischen Fahrzeugen ausgetauschte personenbezogene Daten ausschließlich für Zwecke der Verkehrssicherheit und des Verkehrsmanagements verarbeitet werden dürfen. Insbesondere eine Erhebung zur Bestimmung des Fahrverhaltens darf nur direkt bei den Betroffenen und mit deren Zustimmung erfolgen. Soweit die Kommunikation unmittelbar zwischen Fahrzeugen stattfindet, muss diese nach dem Stand der Technik einen effektiven Schutz vor zweckfremder Verwendung der ausgetauschten Daten bieten. Rechtmäßige Zugriffe auf Daten in Fahrzeugen jenseits einer informierten Einwilligung sollten nach dem Vorbild des Smart Meter Gateway durch einen vertrauenswürdigen Dritten vermittelt werden.

- Datenschutz und Datensicherheit bei Verbrauchsmessungen ausbauen

  Für den Bereich der Messung elektrischer Energie wurde mit dem Smart Meter Gateway eine Lösung geschaffen, die ein hohes Niveau an Cybersicherheit und Datenschutz gewährleistet. Dieses Schutzniveau muss auch für weitere Verbrauchsmessungen in privaten Haushalten, wie etwa Heizwärme- oder Wasserverbrauchsmessung, gelten. Verbrauchs- bzw. Messwerte, die fortlaufend erfasst und weitergeleitet werden können, ermöglichen tiefe Einblicke in die besonders schützenswerte häusliche Privatsphäre.

- Künstliche Intelligenz nicht ohne Grenzen

  Im Bereich Künstlicher Intelligenz (KI) stellen sich zahlreiche grundsätzliche ethische Fragen, auch im Kontext des Datenschutzes. Sicher ist: Es wird Grenzen und Redlichkeitsanforderungen für KI und damit einen klaren Rechtsrahmen geben müssen. Der Gesetzgeber ist aufgerufen, zügig gesetzliche, möglichst gesamteuropäische Regelungen mit klaren Vorgaben für die Gestaltung, den Einsatz und den Umgang mit KI-Systemen auf den Weg zu bringen. So braucht es etwa für den Bereich von Profilbildung und Scoring einer wirksamen Regulierung, die einen klaren Rechtsrahmen und insbesondere mehr Transparenz schafft. Der Lauterkeits-Ansatz der DSGVO, dass niemand einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung mit einer erheblichen rechtliche Wirkung oder Beeinträchtigung unterworfen werden darf, muss fortentwickelt werden und schon den Verarbeitungsprozess untersagen, wenn keine Rechtsgrundlage dafür besteht. Neben einer effektiven und unabhängigen Aufsicht bedarf es auch eines

klaren Sanktionsregimes. Bei entsprechender Ausstattung stehen die Datenschutzaufsichtsbehörden hierzu bereit.

- Messenger ‚Made in Europe'

  Viele populäre Messenger-Apps sind aus Datenschutzsicht bedenklich, obwohl sie einen immer größeren Teil der Kommunikation abdecken. Eine Verschlüsselung der Inhalte allein reicht nicht aus. Es werden Metadaten erhoben und weiterverarbeitet, die über Nutzenden sehr viel aussagen können. Unternehmen und Behörden suchen oft verzweifelt nach geeigneten Alternativen. Es ist höchste Zeit, in Deutschland und Europa datenschutzfreundliche Messenger zu entwickeln und zu etablieren. Die Bundesregierung sollte hier mit gutem Beispiel vorangehen: Deutschland könnte mit Frankreich bei der Etablierung eines Messengers auf Open-Source-Basis kooperieren, damit die Bediensteten – auch im Homeoffice – unkompliziert und zugleich datenschutzkonform kommunizieren können[1]. In einem zweiten Schritt könnte dieser Messenger für alle Bürgerinnen und Bürger geöffnet werden. Offene Schnittstellen schaffen Interoperabilität und ermöglichen die Kommunikation mit Nutzerinnen und Nutzern anderer Dienste. Wo es notwendig ist, sollte Interoperabilität gesetzlich verpflichtend werden.

- Einfache Datenverwaltung durch Personal Information Management Systeme

  Viele Nutzende möchten ihre Daten bei verschiedenen Anbietern möglichst einfach verwalten. Die Datenethikkommission hat in diesem Zusammenhang „Personal Information Management Systeme" (PIMS) vorgeschlagen. Die Bundesregierung hat dieses Konzept inzwischen aufgegriffen. Es sollten jetzt konkrete gesetzliche Regelungen zu den Aufgaben und Rechten der Nutzenden geschaffen werden. PIMS sollten zudem auch Vorkehrungen für den Fall der Insolvenz / Auflösung treffen müssen, sofern Daten bei ihnen selbst gespeichert werden (insbesondere „Datentreuhänder"). Nicht passieren darf, dass die Daten dann gelöscht werden oder die Betroffenen keinen Zugriff mehr haben. Auch sollte eine Kooperationsverpflichtung geregelt werden, da PIMS ins Leere laufen, wenn es keine entsprechenden Schnittstellen gibt.

- ePrivacy-VO – Mit hohen Datenschutzstandards endlich zu einem Ergebnis

  Sollten die seit Anfang 2017 andauernden Verhandlungen zur ePrivacy-Verordnung auf EU-Ebene auch bis zur Bundestagswahl 2021 noch immer nicht abgeschlossen sein, kommt die Politik nicht umhin, sich hierzu nochmals ausdrücklich

[1] Die Bundeswehr hat sich bereits entschieden, auf die gleiche Technik zu setzen wie der französische Staat, also einen Messenger auf Basis von Matrix zu entwickeln/nutzen

zu positionieren: Es braucht endlich passgenaue und zeitgemäße Regeln digitaler Kommunikation. Die neuen Vorschriften dürfen auf keinen Fall hinter das bewährte, hohe Schutzniveau der DSGVO zurückfallen. Vielmehr muss ein hohes, kommunikationsspezifisches Schutzniveau sichergestellt sein, das die informationelle Selbstbestimmung von Verbrauchern und Endnutzern in den Mittelpunkt stellt. Um über das Schutzniveau der aktuellen ePrivacy-Richtlinie hinauszugehen, sollte sich die ePrivacy-Verordnung dabei am Vorschlag der EU-Kommission vom Januar 2017 orientieren. Besonders wichtig ist die künftige Aufsicht über die Einhaltung der Verordnung: Diese sollte für alle datenschutzrechtlichen Vorschriften beim BfDI und den anderen europäischen Datenschutzbehörden angesiedelt sein. Denn nur, wenn auch die Aufsicht über spezielle Datenschutzvorschriften nach e-Privacy-Verordnung bei den Datenschutzbehörden liegt, ist eine einheitliche Anwendung von DSGVO und ePrivacy-Verordnung möglich.

- Digitale Gesundheit – nicht ohne Datenschutz

  Die Digitalisierung im Gesundheitswesen hat nach jahrelangen Verzögerungen nun doch endlich erheblich Fahrt aufgenommen. Diese Entwicklung kann viele Vorteile bringen – für Patientinnen und Patienten, Medizinpersonal, Pflegekräfte, Kostenträger und die Gesellschaft allgemein. Angesichts der umfassenden Verarbeitung sensibler Gesundheitsdaten muss allerdings sichergestellt sein, dass es zu keinem Missbrauch durch private oder staatliche Stellen, zu Stigmatisierungen oder Profilbildungen kommen kann. Von entscheidender Bedeutung ist zudem die grundsätzliche Vorgabe, dass die Kontrolle über ihre Daten in den Händen der Versicherten liegt. Angesichts der Sensibilität von Datenverarbeitungen im Gesundheitsbereich sollte der Gesetzgeber insgesamt Transparenz, Kontrolle und Schutz sensibler Verarbeitungen schärfen. Telematikbasierte Versicherungsmodelle sollten eng reglementiert werden.

- Patientendaten-Schutz-Gesetz überarbeiten

  Gerade im Hinblick auf die elektronische Patientenakte, die zum 1. Januar 2021 eingeführt werden soll, muss die Patientensouveränität für alle Versicherten, auch für diejenigen, die keine mobilen Geräte nutzen können oder wollen, uneingeschränkt gewährleistet sein. Dies ist bei den Regelungen im Patientendaten-Schutz-Gesetz derzeit aber nicht der Fall. Sie stehen zum Teil im Widerspruch zur DSGVO und sind damit europarechtswidrig.

- Datenschutzkonformes Messaging im Gesundheitswesen

  Bekannte datenschutzrechtliche Probleme bei der Nutzung populärer Messenger-Apps bestehen in noch größerem Maße bei der Nutzung dieser Apps im Gesundheitsbereich, da hier über unsichere Kommunikationswege höchstsensible Gesundheitsdaten übermittelt werden. Gerade deshalb ist es beispielsweise besonders wichtig, dass eine Kommunikation nur auf der Grundlage einer verlässlichen Identifizierung und Authentifizierung der Kommunikationspartner erfolgt. Auch was den Gesundheitsbereich anbelangt, bedarf es zügig datenschutzkonformer Alternativen zum bisher gängigen Angebot.

- Datenschutz in der Gesundheitsforschung

  Forschung mit Gesundheitsdaten ist für die Weiterentwicklung in der Medizin unabdingbar. Dies darf aber nicht dazu führen, im Forschungsbereich den Schutz gerade dieser besonders schützenswerten Daten zu vernachlässigen. Die DSGVO sieht hier vor, die Persönlichkeitsrechte der betroffenen Personen bei Forschungsvorhaben durch geeignete technische und organisatorische Maßnahmen sicherzustellen. Soweit es nur geht, sollte Forschung im Gesundheitsbereich zudem mit anonymisierten Daten erfolgen und nur dort, wo dies nicht möglich ist, dürfen sichere Pseudonyme genutzt werden. Angesichts der Sensibilität der Daten einerseits und der Bedeutung der wissenschaftlichen Forschung für den medizinischen Fortschritt andererseits, ist ein Forschungsdatenschutzgesetz notwendig, um Rechtssicherheit zu schaffen.

- Ein Beschäftigtendatenschutzgesetz muss her

  Der digitale Wandel vollzieht sich auch in der Arbeitswelt rasant. Mit der Digitalisierung ihres Arbeitsumfelds steigt für Beschäftigte aber zugleich das Risiko, ihre Privatsphäre bis hin zu einer totalen Überwachung einzubüßen. An vielen Stellen sind sie zunehmend mit neuen Technologien konfrontiert, ohne dass es hierfür einen spezifischen Rechtsrahmen gäbe: Künstliche Intelligenz im Bewerbungsverfahren, Screening von Beschäftigten, GPS-Tracking oder Videoüberwachung – nur einige exemplarische Herausforderungen der Digitalisierung der Arbeitswelt, die Regelungslücken sichtbar und einen besseren Schutz wichtiger denn je machen. Dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit herrscht, verdeutlichen auch immer wieder Datenskandale. Daher braucht es ein Beschäftigtendatenschutzgesetz, das spezifische Verarbeitungen im Beschäftigtenkontext und insbesondere Eckpunkte, wie beispielsweise ein Verbot der Totalüberwachung, Grenzen einer Verhaltens- und Leistungskontrolle, Beweisverwertungsverbote sowie den Einsatz neuer Technologien, regelt. Neben

einer starken Datenschutzaufsicht braucht es dabei auch Instrumente individuellen und kollektiven Schutzes, z. B. durch Mitbestimmungs- und Offenlegungspflichten.

- Prozessrecht

  Datenschutzrechtliche Verarbeitungsverbote ziehen nicht zwangsläufig prozessuale Verwertungsverbote nach sich. Insbesondere im Zivilprozess sowie speziell bei arbeitsrechtlichen Auseinandersetzungen greift der datenschutzrechtliche Schutz zu kurz, wenn rechtswidrig erlangte bzw. verarbeitete Informationen gleichwohl gegen Betroffene verwendet werden können. Daher sollte das Prozessrecht dahingehend überprüft werden, inwieweit datenschutzrechtliche Verwertungsverbote im Sinne der Einheit der Rechtsordnung rechtsstaatlich geboten sind.

II. Öffentliche Verwaltung

- Kein universelles Personenkennzeichen

  Ein modernes Land braucht eine moderne Verwaltung, die es auf digitalem Weg erlaubt, von zu Hause aus online Anträge zu stellen und weitere Verwaltungsleistungen abzurufen. Allerdings braucht es dafür kein einheitliches, verwaltungsübergreifendes Personenkennzeichen oder sonstige Identifikatoren, wie etwa die Steuer-ID. Bereichsspezifische Kennzeichen sind ebenso geeignete Alternativen, die den großen Vorteil bieten, die Möglichkeit der rasanten Zusammenführung aller Daten zu einer Person wirkungsvoll auf ein verfassungsrechtlich erträgliches Maß zu reduzieren. Und auch für den Registerzensus gilt: Die datenschutzrechtliche Verbesserung, künftig auf unmittelbaren Befragungen zu persönlichen Verhältnissen zu verzichten, wird zunichte gemacht, wenn Informationen verschiedener Register über ein universelles Personenkennzeichen miteinander verknüpft werden und zudem neue Register geschaffen werden müssen, um etwa die erforderliche Datenqualität zu gewährleisten.

- Whistleblower-Richtlinie schnell und effizient umsetzen!

  Der Whistleblower-Schutz ist unabdingbar, um Missstände in Wirtschaft und Verwaltung offenzulegen. Dieser zeitgemäßen Sichtweise trägt die Whistleblower-Richtlinie der EU (2019/1937/EU) Rechnung. Sie ist bis Ende 2021 in deutsches Recht umzusetzen und dient auch dem Schutz redlicher Hinweisgebenden, soweit es um die Einhaltung datenschutzrechtlicher Bestimmungen geht. Ihre Umsetzung sollte unter Wahrung höchstmöglicher Datenschutzstandards für sowohl Hinweisgebende, mutmaßlich Verantwortliche, als auch Zeugen und Dritte schnellstmöglich erfolgen. Die Bündelung verschiedener Sachbereiche bei einer

Meldestelle, die Ermöglichung auch anonymer Hinweise sowie der Schutz der Identität von Hinweisgebern und die Sicherstellung absoluter Vertraulichkeit der Hinweise zählen zu den grundlegenden Anforderungen. Die Errichtung der in der Richtlinie zwingend vorgesehenen externen Anlaufstelle sollte daher beim BfDI als unabhängiger oberster Bundesbehörde in einer gesonderten Einheit erfolgen.

III. Sicherheit

- Technischer Datenschutz – ein Schlüssel zu mehr Sicherheit

  Bildung, Forschung und Förderung im Bereich des technischen Datenschutzes greifen deutlich zu kurz, obwohl sie ein entscheidender Baustein zu mehr IT-Sicherheit sind. Hier ist dringend ein neuer und nachhaltiger Ansatz gefragt. Privacy by Design und Privacy by Default müssen mehr denn je zu festen Bestandteilen bei der Entwicklung und Gestaltung von Anwendungen werden. Leider ist es bisher nicht gelebte Praxis, Technologien und Prozesse bereits von Beginn an so zu entwickeln und zu gestalten, dass datenschutzrechtliche Vorgaben umgesetzt und somit zu einer Selbstverständlichkeit bei der Nutzung von Informations- und Kommunikationstechnik werden. Einfache und sichere kryptografische Systeme und Verschlüsselungstechniken, die von jedermann eingesetzt werden können, sind solche zentralen Technologien, die verstärkt Einzug in unseren Alltag finden müssen. Dies auch, weil Vertrauen in die Sicherheit digitaler Angebote essentiell ist. Deswegen kann und darf der Staat dies nicht unterminieren, indem er verpflichtende Hintertüren fordert, die zwangsläufig auch Dritten offen stehen. Stattdessen sollten öffentliche Stellen den Einsatz von Verschlüsselungstechniken voranbringen, etwa indem sie Bürgerinnen und Bürgern verschlüsselte E-Mails als Kommunikationskanal anbieten müssen.

- Anonymisierungsverfahren nutzen

  Zu jenen Technologien, die künftig stärker gefördert werden müssen, gehören auch Anonymisierungsverfahren. Sie ermöglichen in vielen Fällen eine umfassende Datennutzung ohne negative Datenschutzimplikationen. Dabei sollten Standards zur Anonymisierung von Daten festgelegt und fortwährend an den technologischen Fortschritt angepasst werden. Um Vertraulichkeit und Integrität informationstechnischer Systeme dauerhaft zu gewährleisten, ist der Gesetzgeber gut beraten, einen entsprechenden Rechtsrahmen zu schaffen, der auch schnellen Veränderungen Rechnung trägt.

- Sicherheitsgesetz-Moratorium überfällig

  Immer wieder fordern Teile der Politik und der Sicherheitsbehörden geradezu reflexartig schärfere Sicherheitsgesetze mit mehr Aufgaben und Befugnissen, wenn es darum geht, schnell Antworten auf Ereignisse und Bedrohungslagen zu geben. Den Erfolg einer Sicherheitsarchitektur kennzeichnet aber nicht die Summe der Sicherheitsgesetze oder die Zahl der Eingriffsbefugnisse, sondern die tatsächliche Effizienz jeder einzelnen Maßnahme im Vollzug. Gefragt ist also eine vorausschauende passgenaue Sicherheitsarchitektur. Vollzugsdefizite, die auf fehlenden sachlichen oder personellen Ressourcen beruhen, lassen sich nicht durch weitere Sicherheitsgesetze kompensieren. Deswegen sollte es auch im Interesse der Sicherheitsbehörden sein, die eigenen Sicherheitsgesetze unter Effizienzgesichtspunkten regelmäßig zu evaluieren, überflüssigen Ballast loszuwerden und die eigenen Ressourcen zu konzentrieren. Ungeeignete oder überflüssige Grundrechtseingriffe sind rechtswidrige Beschränkungen von Freiheit. Selbst wenn ein einzelner Eingriff für sich isoliert betrachtet noch verhältnismäßig sein mag, muss auch die Überwachungsgesamtlast, die Bürgerinnen und Bürger trifft, im Wege einer Gesamtschau ebenso noch verhältnismäßig sein. Nachdem in den letzten Jahren die Zahl der Sicherheitsgesetze bzw. deren Verschärfungen stets zugenommen haben, ohne das gleichzeitig an anderer Stelle das Überwachungsmaß reduziert worden wäre, sich die technologischen Möglichkeiten erweitert und der Umfang zu erhebender Daten sich vervielfacht haben, ist es nun an der Zeit für ein Sicherheitsgesetz-Moratorium mit einer Überwachungsgesamtrechnung.

- Keine anlasslose und flächendeckende Vorratsdatenspeicherung

  Das Thema Vorratsdatenspeicherung polarisiert. Befürworter einer anlasslosen und pauschalen Vorratsdatenspeicherung fordern, dass das, was technisch möglich ist, auch rechtlich erlaubt sein sollte. Sie berufen sich auf die Notwendigkeit solcher Datensammlungen für Ermittlungs- und Sicherheitsbehörden, um Straftaten aufzudecken und Bedrohungen abzuwehren. Dem gegenüber gibt es aber auch viele Stimmen, die eine anlasslose Vorratsdatenspeicherung kritisieren, ihren Nutzen bezweifeln und gleichzeitig Freiheiten und Bürgerrechte bedroht sehen. In diesem Sinne äußert sich auch der BfDI seit Jahren zu dem Thema Vorratsdatenspeicherung: Es muss auch in Zeiten fortschreitender Digitalisierung möglich sein, dass rechtschaffene und unbescholtene Bürgerinnen und Bürger im Internet oder mittels moderner Kommunikationsmittel kommunizieren können, ohne eine ausufernde Speicherung und Auswertung ihrer Kommunikationsdaten befürchten zu müssen. Jede Regelung zur Vornahme der Speicherung von Kommunikationsdaten muss deshalb anlassbezogen, zeitlich und im Umfang befristet

sein und einer wirksamen Überprüfung durch ein Gericht oder einer unabhängigen Verwaltungsbehörde unterliegen.

- Datenschutz auch im Polizeibereich durchsetzen

  Polizeibehörden verarbeiten häufig besonders sensible Daten über Bürgerinnen und Bürger. Doch ausgerechnet hier fehlen der Datenschutzaufsicht größtenteils wirksame Durchsetzungsbefugnisse. Einzig gegenüber dem BKA kann der BfDI verbindliche Maßnahmen anordnen, sofern er einen Datenschutzverstoß beanstandet hat und die Anordnung zur Beseitigung dieses Verstoßes erforderlich ist. Ansonsten können gegenüber Polizei- und Strafverfolgungsbehörden weiterhin keine verpflichtenden Anordnungen getroffen, sondern festgestellte Verstöße nur unverbindlich beanstanden werden. Dies widerspricht dem klaren Wortlaut der maßgeblichen europarechtlichen Regelungen. Zudem kann so keine gerichtliche Prüfung eingeleitet werden. Der BfDI ist daher mit wirksamen Abhilfebefugnissen nach EU-Recht auszustatten.

- Möglichkeiten der Nachrichtendienste-Kontrolle ausbauen

  Heimliche Grundrechtseingriffe, wie sie üblicherweise insbesondere von Nachrichtendiensten getätigt werden, kennzeichnet, dass die Betroffenen in der Regel davon nichts erfahren. Damit fehlt ihnen die Möglichkeit, Maßnahmen gerichtlich überprüfen zu lassen. Das Bundesverfassungsgericht hat in mehreren Entscheidungen klargestellt, dass ein wichtiger Aspekt bei der Frage, ob ein Eingriff verfassungsgemäß ist, eben auch sei, ob der fehlende Rechtsschutz durch eine effektive (Datenschutz-) Kontrolle kompensiert werde. Genau hier hat der Gesetzgeber jedoch bisher nicht ausreichend nachgearbeitet. So führt eine bloße Beanstandung durch den BfDI in der Regel nur zur Feststellung eines Dissenses, wobei die Nachrichtendienste anschließend weiterhin unverändert an ihrer Praxis festhalten können, weil sie sich keiner weitergehenden – insbesondere keiner gerichtlichen – Überprüfung ausgesetzt sehen. Zudem erschweren sie ihre Kontrolle, indem sie Zuständigkeiten der verschiedenen Kontrollorgane gegeneinander ausspielen.
  Wer eine effektive Durchsetzung des Datenschutzes im Bereich der Nachrichtendienste will, muss die Befugnisse der Datenschutzaufsicht deutlich ausbauen. Dies heißt ein umfassendes proaktives Berichtswesen gegenüber der Aufsicht sowie die Möglichkeit, festgestellte Datenschutzverstöße zu unterbinden. Nachrichtendienste sollten ihrerseits Anweisungen gerichtlich überprüfen lassen können. Weiterhin sollte die Berechtigung und Verpflichtung zu Austausch und umfassender Kooperation aller Aufsichtsorgane im Bereich der Nachrichtendienste gesetzlich verankert und ausgestaltet werden.

IV. Datenschutzrecht und Aufsicht

- DSGVO 2.0 – den Erfolg fortschreiben

  Die DSGVO ist ein Erfolg. Trotzdem hat sich an der einen oder anderen Stelle auch deutlicher Nachbesserungsbedarf gezeigt. Entscheidend für das Funktionieren und die Akzeptanz der DSGVO ist das Verfahren der Kohärenz und Zusammenarbeit der europäischen Aufsichtsbehörden im Europäischen Datenschutzausschuss. Bei der Durchsetzung der DSGVO insbesondere gegenüber großen internationalen Internetunternehmen hat sich allerdings gezeigt, dass das bisherige Verfahren mit einer starken Rolle der federführenden Aufsichtsbehörde am europäischen Hauptsitz des Unternehmens erhebliche Defizite aufweist. Wichtige Fälle sollten deshalb direkt dem Europäischen Datenschutzausschuss zugeteilt werden, der hierzu allerdings eine Arbeitsebene benötigt. Weitere zu schließende Lücken in der DSGVO betreffen besondere Verarbeitungen, bei denen der allgemeine und technikneutrale Ansatz der DSGVO zu kurz greift. Dies gilt etwa beim Scoring und Profiling, aber auch bei Big Data, Künstlicher Intelligenz und anderen algorithmenbasierten Entscheidungen. Hierbei fehlt es an Regelungen, die gezielt von manipulativen und diskriminierenden Verarbeitungen spezifisch schützen. Auch sollten profilbildende Verarbeitungen an sich bereits reglementiert werden, nicht erst der Umgang mit Ergebnissen dieser Prozesse. Was die Kritik am mit der DSGVO einhergehenden bürokratischen Aufwand für kleine Unternehmen und Vereine angeht, so lassen sich einzelne Pflichten vertretbar reduzieren, ohne Datenschutzinteressen zu opfern. Dies gilt etwa für die Informationspflichten nach den Art. 13 und 14 DSGVO. In bestimmten Fällen könnten Informationspflichten zudem künftig nur noch auf Verlangen greifen. Dies beträfe etwa Datenverarbeitungen, die erwartbar und nicht risikobehaftet sind. Das Bundesdatenschutzgesetz muss zudem überarbeitet werden, um europarechtswidrige Vorschriften, wie die zur Videoüberwachung öffentlich zugänglicher Räume in § 4 BDSG, zu streichen.

- Die Potentiale der Datenschutzkonferenz nutzen

  Die Zusammenarbeit der deutschen Aufsichtsbehörden im Rahmen der Datenschutzkonferenz (DSK) sollte weiter verbessert werden, auch um eine Harmonisierung sicherzustellen. Zur Stärkung der DSK und zur koordinierenden Unterstützung gerade der kleineren Landesdatenschutzbeauftragten sollte die DSK eine permanente Geschäftsstelle erhalten. Der BfDI ist bereit, zur Erreichung der genannten Ziele anknüpfend an seine Funktion als gemeinsamer Vertreter im Europäischen Datenschutzausschuss und unter Einbeziehung der in seinem Haus angesiedelten Zentralen Anlaufstelle noch stärker als bisher eine Schnittstellenfunktion im Kreis der Aufsichtsbehörden zu übernehmen.

V. Transparenz

- Informationsfreiheit fortentwickeln

  Transparenz ist ein zentraler Faktor für die Akzeptanz staatlichen Handelns. Das Informationsfreiheitsgesetz (IFG) sollte deshalb zu einem Transparenzgesetz weiterentwickelt werden, in das die Ergebnisse der erfolgten Evaluierung einfließen. Mit der proaktiven Veröffentlichung von Informationen kann Vertrauen in staatliche Entscheidungen gestärkt und Falschinformationen frühzeitig begegnet werden.

- Ausnahmetatbestände beim Informationsfreiheitsgesetz kritisch prüfen

  Die bestehenden Ausnahmetatbestände sollten kritisch auf Redundanz und ihre Notwendigkeit geprüft werden. Um die Bedeutung des Informationszugangs in der Demokratie zu stärken, sollte ein „public interest test“ eingeführt werden. Das würde bedeuten, dass nicht nur das individuelle Interesse am Informationszugang und das Geheimhaltungsinteresse in die jeweilige Abwägung einfließen, sondern in einem weiteren Schritt geprüft werden muss, ob ein relevantes öffentliches Interesse an der Veröffentlichung einer Information besteht.

- Vereinheitlichung der Informationsrechte

  Das Verbraucherinformationsrecht sollte wie das Informationsfreiheitsrecht und – derzeit im Bundestag beraten – das Umweltinformationsrecht eine Unterstützung der Bürgerinnen und Bürger sowie der Behörden durch den BfDI vorsehen. Mittelfristig sollten die drei zugrundeliegenden Informationszugangsgesetze in einem Transparenzgesetz zusammengeführt werden.

- Verbindliche Anordnungen und weitere Sanktionen

  Um die Antragstellerinnen und Antragsteller bei der Durchsetzung ihrer Rechte unterstützen zu können, sollte der BfDI in den Informationszugangsgesetzen die Möglichkeit für verbindliche Anordnungen und weitere Sanktionen analog zu den bestehenden datenschutzrechtlichen Befugnissen erhalten. Damit wären Antragstellerinnen und Antragsteller nicht mehr nur auf den zeit- und kostenintensiven Weg des gerichtlichen Rechtsschutzes angewiesen.