Bundesministerium
des Innern, für Bau
und Heimat

eu2020.de

Bundesministerium des Innern, für Bau und Heimat, 11014 Berlin

vorab per Telefax: 0721/9101-382

Präsidenten des Bundesverfassungsgerichts
Herrn Professor Dr. Harbarth, LL.M.
Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

Dr. Helmut Teichmann
Staatssekretär

Alt-Moabit 140
10557 Berlin
Postanschrift
11014 Berlin

Tel. +49 30 18 681-11112
Fax +49 30 18 681-511112

STT@bmi.bund.de

www.bmi.bund.de

Berlin, 29. September 2020

Betreff: Stellungnahme der Bundesregierung in den Verfahren 1 BvR 2771/18 gegen § 23b Abs. 2 i.V.m. Abs. 1 PolG BW und 1 BvR 1552/19 gegen die §§ 15b, 15c HSOG.

Bezug: Ihre Schreiben vom 15. und 17. April 2020

Sehr geehrter Herr Präsident,

namens der Bundesregierung nehme ich zu den in den Übermittlungsschreiben vom 15. und 17. April 2020 aufgeworfenen Fragen,

(1) ob eine verfassungsrechtliche Notwendigkeit staatlicher Maßnahmen zum Schutz informationstechnischer Systeme gegen Dritte gesehen wird,

(2) ob solche Schutzvorschriften bestehen und

(3) ob in diesem Zusammenhang VO (EU) Nr. 2016/679, RL (EU) Nr. 2016/680 und den diesbezüglichen Vorschriften des deutschen Rechts Bedeutung beigemessen wird

wie folgt Stellung:

(1) Verfassungsrechtliche Notwendigkeit staatlicher Maßnahmen zum Schutz informationstechnischer Systeme gegen Dritte

Aus Sicht der Bundesregierung ist das bestehende Regulierungssystem zur Gewährleistung der IT-Sicherheit und des Datenschutzes in Deutschland mit Blick auf das Spannungsverhältnis zwischen Gewährleistung von IT-Sicherheit einerseits und Erfüllung des gesetzlichen Auftrags der Strafverfolgungs- und Sicherheitsbehörden andererseits notwendig, aber auch ausreichend.

Das Bundesverfassungsgericht hat festgestellt, dass „aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, ein grundrechtlich erhebliches Schutzbedürfnis [folgt und] der Einzelne darauf angewiesen [ist], dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet." (BVerfGE 120, 274 <306>)

Allerdings gilt auch das im Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG fußende und seit der o.g. Entscheidung als solches bezeichnete Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht schrankenlos. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. (BVerfGE 120, 274 <315>)

Eingriffe meint vor diesem Hintergrund jedoch Eingriffe in die abwehrrechtliche Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, um die Freiheitssphäre des Einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern.

Die Frage nach einer möglicherweise bestehenden, verfassungsrechtlichen Notwendigkeit von Schutzmechanismen betrifft eine objektivrechtliche Schutzverpflichtung. Diese Dimension der Grundrechte besteht darin, dass sie als objektive Prinzipien staatliche Schutzpflichten begründen und dadurch ihre prinzipielle Geltungskraft für Staat und Gesellschaft verstärken.

Die sich aus dem objektiven Gehalt der Grundrechte ergebenden staatlichen Schutzpflichten führen regelmäßig nicht zu einem Anspruch auf einen bestimmten Schutz. Sie verpflichten den Staat, einen angemessenen Schutz vor Beeinträchtigungen durch Dritte zu begründen und durchzusetzen sowie sich für ein effizientes Schutzregime einzusetzen und sind vorrangig ein zielorientiertes Handlungsprogramm für den Gesetzgeber, das in erster Linie durch das Untermaßverbot begrenzt ist.

Der Staat muss seiner grundrechtlichen Schutzpflicht gegenüber Grundrechtsbeeinträchtigungen beispielsweise durch ausländische Staaten und deren Institutionen oder durch private, häufig global operierende Unternehmen oder Privatpersonen mittels hin-

reichender Vorkehrungen genügen. Allerdings kann aus dem Verfassungsrecht regelmäßig keine bestimmte Handlungsvorgabe abgeleitet werden, sondern entfalten die Freiheitsrechte hier nur eine Wirkung als Verbot eines Untermaßes an staatlichem Schutz (Papier, NJW 2017, 3025 <3030>). Der grundrechtliche Schutzanspruch ist nur darauf gerichtet, „dass die öffentliche Gewalt Vorkehrungen zum Schutze des Grundrechts trifft, die nicht gänzlich ungeeignet oder völlig unzulänglich sind." (BVerfGE 77, 170 <214 f.>). Noch konkreter kommt ein Verstoß insofern erst dann in Betracht, „wenn Schutzvorkehrungen entweder überhaupt nicht getroffen sind, wenn die getroffenen Regelungen und Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder wenn sie erheblich hinter dem Schutzziel zurückbleiben" (BVerfGE 125, 39 <78 f.>).

Für den hier interessierenden Zusammenhang ist zu berücksichtigen, dass die Versorgung der Öffentlichkeit mit IT-Systemen nicht durch den Staat erfolgt, sondern Privaten überlassen ist. Die staatliche Systemverantwortung kommt damit nur komplementär zum Tragen: Telekommunikations-/Telemedienunternehmen, IT-Anbieter und Hardware-Hersteller haben ein eigenes Interesse an einem Fehlermonitoring, um ihre Produkte und Kunden vor Angriffen zu schützen. Weil der Staat grundsätzlich auf diese privatwirtschaftliche Fehlerbeseitigung vertrauen darf, sind weiterreichende Schutzverpflichtungen im Sinne eines staatlichen Monitorings sämtlicher Systeme und ihrer Sicherheitslücken durch staatliche Stellen nicht geboten.

Dem System grundrechtlicher Schutzpflichten ist immanent, dass sie ein Rechtsgebot zum Eingriff in Rechte Dritter zu Gunsten eines anderen Grundrechtsträgers aufstellen können. Im Zusammenwirken von Demokratie- und Rechtsstaatsprinzip lässt sich insoweit eher an politische Verantwortungszusammenhänge denken, weshalb der Gesetzgeber hier grundsätzlich über einen Einschätzungs-, Wertungs- und Gestaltungsspielraum verfügt (Maunz/Dürig-di Fabio, Grundgesetz-Kommentar, 90. EL 2020, Art. 2 Abs. 1 GG, Rn. 61, 135), innerhalb dessen er Abwehr- und Schutzpflichtendimension der Grundrechte in einen Ausgleich bringen kann (BVerfGE 46, 160 <164>; 96, 56 <64>). Für eine Schutzverpflichtung in dem Umfang, wie sie für das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nur angelegt sein kann, kann nichts anderes gelten.

Neben dem Schutz informationstechnischer Systeme spielt in diesem Kontext die Nutzung von IT-Schwachstellen[1] und Exploits[2] zum Zwecke der Durchsetzung bestehender Befugnisse etwa im Rahmen der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) oder der Onlinedurchsuchung zum Schutz überragend wichtiger anderer Rechtsgüter eine wichtige Rolle.

Moderne Softwareprodukte (und auch Hardwareprodukte) enthalten in der Regel eine Vielzahl an bekannten und unbekannten sog. Schwachstellen. Solche Schwachstellen ermöglichen verdeckte, aber auch öffentlichkeits-wirksame Cyberangriffe auf Privatpersonen, öffentliche Institutionen, kritische Infrastrukturen oder privatwirtschaftliche Unternehmen. Wenngleich wegen der Komplexität heutiger Softwareentwicklungsprozesse und angesichts der rasanten Innovationszyklen in der heutigen IT-Entwicklung „fehlerfreie Software" auf lange Sicht de facto nicht erreichbar sein wird, ist vom Standpunkt der IT-Sicherheit - nicht nur auf Seiten der Hersteller - dennoch eine möglichst geringe Zahl an offenen Schwachstellen in allen IT-gestützten Geräten anzustreben.

Aufgrund der immer stärker verbreiteten Nutzung von Ende-zu-Ende-Verschlüsselung (z.B. durch bekannte Messenger wie WhatsApp, Signal, Telegram oder Threema), die gezielt verwendet werden, um Tat- oder Kommunikationsmittel bewusst einem Zugriff durch Strafverfolgungs- und Sicherheitsbehörden zu entziehen, bestehen hinsichtlich einer Kommunikationsüberwachung oftmals keine anderen erfolgversprechenden technischen Möglichkeiten als durch die Nutzung von Schwachstellen auf die jeweiligen Endgeräte zu gelangen und dort die unverschlüsselte Kommunikation auszulesen.

Bestehende rechtliche Befugnisse zur Quellen-TKÜ und Onlinedurchsuchung würden ohne eine Nutzungsmöglichkeit von Schwachstellen in einer Vielzahl von Fällen schlichtweg ins Leere laufen.

---

[1] Eine **Schwachstelle** ist definiert als eine Sicherheitslücke in Soft- oder Hardware, die einzeln oder kombiniert genutzt werden kann, um (in der Regel unbemerkt) aktiven Zugriff auf ein Hard- oder Softwaresystem zu erhalten. Man unterscheidet zwischen sogenannten Zero-Day (auch 0-day) und sogenannten n-Day Sicherheitslücken. Zero-Day-Sicherheitslücken sind bisher weder Öffentlichkeit noch dem Hersteller bekannt, so dass weder Software-Updates für die Schließung der Sicherheitslücken existieren und auch keine entsprechenden Signaturen für eine Erkennung durch Virenscanner o.Ä. existieren. Zero-Day meint daher wörtlich „0 Tage bekannt". n-Day-Sicherheitslücken hingegen wurden dem Hersteller gemeldet, sind in öffentlichen Verzeichnissen gelistet und können somit prinzipiell erkannt und beseitigt werden. n-Day meint daher wörtlich „n Tage bekannt". Naturgemäß benötigten die Hersteller mehrere Tage bis Wochen bevor ein entsprechendes Update die Schwachstelle beseitigt. Daher hat sich die Praxis etabliert, dass professionelle Sicherheitsteams entdeckte Schwachstellen zunächst nur dem Hersteller und erst nach Ablauf einer Frist gegenüber der Allgemeinheit veröffentlichen (sog. Prinzip „responsible disclosure"). Trotz Bereitstellung von Software-Updates bleiben viele n-days noch für Jahre ein Sicherheitsproblem, da durch fehlendes Sicherheitsbewusstsein Updates nicht eingespielt werden. Insbesondere bei Schwachstellen in nicht veränderbarer Hardware oder in Systemen deren Hersteller keine Sicherheitsupdates bereitstellen, stellen n-days ein ebenso großes Risiko wie 0-days dar.

[2] Ein **Exploit** (engl. to exploit: ausnutzen) ist ein Werkzeug oder eine systematische Möglichkeit (auch Beschreibung), um Schwachstellen und Fehlfunktionen von Hard- oder Software auszunutzen, um sich zum Beispiel den Zugriff auf die Daten oder Ressourcen zu verschaffen.

Das Ziel, einerseits größtmögliche IT-Sicherheit zu gewährleisten und andererseits die Notwendigkeit, Strafverfolgungs- und Sicherheitsbehörden die Erfüllung ihres gesetzlichen Auftrags zu ermöglichen, stehen also in einem Spannungsverhältnis zueinander. Dieses Spannungsverhältnis ist innerhalb der oben geschilderten Spielräume des Gesetzgebers und unter Bewahrung des größtmöglichen Schutzes für alle betroffenen Rechtsgüter aufzulösen.

Dieser Zielkonflikt wird durch die Eckpunkte der deutschen Kryptopolitik widergespiegelt: „Sicherheit durch Verschlüsselung" einerseits und „Sicherheit trotz Verschlüsselung" andererseits.

Dies gilt insbesondere vor dem Hintergrund der Gefahr einer Beeinträchtigung des Vertrauens der Bevölkerung in moderne digitale Kommunikationsmittel, wie sie auch das Bundesverfassungsgericht konkret für die Onlinedurchsuchung nach dem nordrhein-westfälischen Verfassungsschutz-gesetz ausgemacht hat:

„Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist."
(BVerfGE 120, 274 <326>)

Im Rahmen ihrer Zuständigkeiten ist Ziel der Bundesregierung, den geschilderten Konflikt ohne eine solche Vertrauensbeeinträchtigung mit größtmöglichem Schutz der Bevölkerung sowohl vor den Gefahren und Rechtsgutbeeinträchtigungen, zu deren Verhütung oder Aufklärung die Quellen-TKÜ und Onlinedurchsuchung genutzt werden, als auch vor solchen Gefahren, die von Schwachstellen in informationstechnischen Systemen ausgehen, aufzulösen.
Es wäre auch deutlich zu kurz gegriffen, die Ausbreitung von Angriffskampagnen (z.B. „WanaCry") auf ein Zurückhalten von Sicherheitslücken durch Staatsorgane zurückzuführen. Spätestens durch das Ausrollen von Sicherheitsupdates entsteht die Situation, dass potentielle Angreifer diese Sicherheitsupdates analysieren und einen Exploit generieren können.

Ausgangspunkt für die Auflösung des vorstehend beschriebenen Konflikts ist das bestehende, nachfolgend unter (2) und (3) skizzierte Regulierungs-system zur Gewährleistung der IT-Sicherheit und des Datenschutzes in Deutschland.

Zu berücksichtigen ist dabei, dass IT-Sicherheit zu einem volkswirtschaftlich entscheidenden Faktor geworden ist. Dabei kommt in erster Linie den Softwareherstellern die Verantwortung zu, weil nur sie – als Hersteller – über das Wissen, die Ressourcen und – aufgrund des Dekompilierungsverbots – über die rechtlichen Möglichkeiten verfügen, Sicherheitslücken zu schließen. Für eine Verantwortungsverlagerung wird keine Notwendigkeit gesehen. Sie wäre auch kontraproduktiv; schon weil die Bundesregierung

durch ihre Behörden, insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI), sowohl Betreiber wie auch Nutzer durch vielfältige Maß-nahmen warnt, informiert und teilweise verpflichtet, sich besonders zu schützen (siehe auch unter (2)).

(2) Vorschriften zum Schutz informationstechnischer Systeme gegen Dritte

Gemäß § 3 Abs. 1 Satz 2 Nr. 2 BSI-Gesetz ist beim BSI die gesetzliche Aufgabe zur Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen angesiedelt.

Nach § 8 c Abs. 3 BSI-Gesetz haben Anbieter digitaler Dienste jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der EU erbrachten digitalen Dienstes hat, unverzüglich an das BSI zu melden.

Nach § 8b Abs. 4 BSI-Gesetz sind Betreiber Kritischer Infrastrukturen verpflichtet, Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen oder führen könnten, dem BSI zu melden. Nach § 10 Abs. 1 BSI-Gesetz erfolgt die Festlegung, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne des BSI-Gesetzes gelten durch die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) des Bundesministeriums des Innern, für Bau und Heimat (BMI).

Ergänzend zu den Regelungen im BSI-Gesetz konkretisiert auch eine Vielzahl spezialgesetzlicher Regelungen die Aufgaben und Verpflichtungen des BSI zum Schutz informationstechnischer Systeme in verschiedenen Bereichen von Staat, Wirtschaft und Gesellschaft. Beispielhaft wird auf die Regelungen im Sozialgesetzbuch Fünftes Buch (SGB V) zur Telematikinfrastruktur verwiesen. Nach § 291 bis § 291h SGB V (nach Inkrafttreten des Patientendaten-Schutz-Gesetzes (PDSG) nach §§ 291 bis 291c SGB V sowie §§ 306 bis 383 SGB V) sind etwa wesentliche technische Festlegungen in Bezug auf die Datensicherheit im Einvernehmen mit dem BSI zu treffen. Dies führt zu hohen Anforderungen an die Entwicklung (Security by Design) und den Betrieb der Anwendungen im Bereich der Telematikinfrastruktur. Für die elektronische Patientenakte findet beispielsweise eine patientenindividuelle Verschlüsselung Anwendung, sodass weder der Betreiber der Akte noch unberechtigte Dritte einen Zugriff auf die hochsensiblen Patientendaten erlangen können.

Weiterhin müssen die Anbieter von Diensten und Komponenten der Telematikinfrastruktur Schwachstellen an die von den Spitzenorganisationen des deutschen Gesundheitswesens zum Zweck der Einführung, Pflege und Weiterentwicklung der elektronischen Gesundheitskarte (eGK) und ihrer Infrastruktur (Telematikinfrastruktur) in Deutschland gegründete gematik GmbH (gematik), an der die Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit, die Mehrheit der Geschäftsanteile hält, melden. Erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser Komponenten und Dienste der Telematikinfrastruktur sind analog den allgemeinen Regelungen zu den Meldepflichten der Betreiber Kritischer

Infrastrukturen durch die gematik an das BSI zu melden. Dies umfasst auch die Meldung von Schwachstellen, die zu entsprechenden Störungen führen könnten.

Mit dem o.g. Ansatz „Sicherheit durch Verschlüsselung" und „Sicherheit trotz Verschlüsselung" strebt die Bundesregierung keine Regulierung oder verpflichtende sonstige Schwächung von Verschlüsselung an, sondern setzt sich für die Verbreitung sicherer Verschlüsselung und die Stärkung des Vertrauens der Nutzer in die Sicherheit der Verschlüsselung ein. Diese Praxis der Bundesregierung ist seit dem Beschluss der Bundesregierung vom 2. Juni 1999 („Eckpunkte der deutschen Kryptopolitik") öffentlich dokumentiert und gilt bis heute unverändert fort.

Bisher wurden für den Umgang mit Schwachstellen bereits Prozesse bezüglich der Meldung innerhalb der Bundesverwaltung an das BSI und durch das BSI etabliert (vgl. § 4 Abs. 2 - 4 BSIG). Demnach müssen grundsätzlich alle Bundesbehörden Informationen im Zusammenhang mit neu festgestellten Schwachstellen, die für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, an das BSI melden.

Gefundene Schwachstellen werden über das BSI dem betroffenen Hersteller gemeldet, damit dieser die Möglichkeit erhält, die Schwachstelle zu schließen. Soweit erforderlich, werden die von der Schwachstelle betroffenen Kreise informiert bzw. gewarnt. Das BSI gibt Schwachstellen nicht an die Sicherheitsbehörden weiter.

Das Verfahren zielt darauf ab, den durch eine mögliche Ausnutzung von Schwachstellen resultierenden Schaden zu minimieren. Zum einen wird durch die koordinierte Beteiligung betroffener Hersteller eine Bereitstellung von funktionierenden Sicherheitsupdates ermöglicht. Zum anderen begrenzt das (nur) temporäre Zurückhalten von Schwachstellen- und Angriffsdetails die Ausnutzung und kann damit das Schadenspotential reduzieren. Als bewährte Methode, sowohl national wie auch international, wird der „Coordinated Vulnerability Disclosure" (CVD) Prozess anerkannt.

Ferner erfolgt der Umgang mit Schwachstellen nach den für die jeweilige Sicherheitsbehörde geltenden gesetzlichen Vorgaben. Es greifen die allgemeinen fachaufsichtlichen und parlamentarischen Kontrollmechanismen sowie die gesetzlich vorgesehenen Rechtsschutzmöglichkeiten.

Um diesen Prozess zu verbessern arbeitet das BMI an einer ausgewogenen behördenübergreifenden Strategie für den Umgang mit Schwachstellen für die Strafverfolgungs- und Sicherheitsbehörden, um auch in Zukunft über bereits vorhandene interne Behördenvorgaben hinaus die Interessen der IT-Sicherheit sowie der Strafverfolgungs- und Sicherheitsbehörden in einen angemessenen Ausgleich bringen zu können. Diese bedarf noch der Abstimmung innerhalb der Bundesregierung.

Unbeschadet dessen stehen derzeit beispielsweise dem Bundeskriminalamt (BKA) im Rahmen seiner gesetzlichen Aufgabe zur Abwehr der Gefahren des internationalen Terrorismus in § 51 Abs. 2 BKAG die Befugnis zur Quellen-TKÜ und in § 49 BKAG die Befugnis zur Online-Durchsuchung unter engen rechtlichen Grenzen zur Verfügung. Neben dem Richtervorbehalt sind diese Maßnahmen an das Erreichen hoher Eingriffsschwellen

gebunden. Hinzu kommen eine zeitliche Begrenzung der Anordnung einer solchen Maßnahme auf grundsätzlich drei Monate, Benachrichtigungspflichten gegenüber den Betroffenen sowie umfangreiche Regelung zur Gewährleistung des Kernbereichsschutzes.

Als verdeckte und eingriffsintensive Maßnahmen unterliegt die Anwendung dieser Befugnisse nicht nur der Kontrolle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (§ 69 BKAG), sondern auch der Berichtspflicht der Bundesregierung gegenüber dem Bundestag (§ 88 BKAG).

(3) Bedeutung von VO (EU) Nr. 2016/679, RL (EU) Nr. 2016/680 und den diesbezüglichen Vorschriften des deutschen Rechts in diesem Zusammenhang

Zur Datenschutz-Grundverordnung – Verordnung (EU) 2016/679 – und den anderen zitierten Vorschriften wird auf Folgendes hingewiesen: Die bestehenden Datenschutzvorschriften sind Teil des Regulierungssystems zum Schutz informationstechnischer Systeme. Außerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung treten weitere datenschutzrechtliche Vorschriften hinzu. Die Bundesregierung geht davon aus, dass die geltenden Regelungen des Datenschutzrechts von allen staatlichen Stellen beachtet werden.

Dies gilt auch für die o.g. unionsrechtlichen Vorgaben und deren Umsetzungsregelungen, die im beschwerdegegenständlichen Kontext Anwendung finden. Die Datenschutz-Grundverordnung verpflichtet die Telekommunikations-/Telemedienunternehmen und IT-Anbieter u.a. mit Art. 25 (sog. „Privacy by Design") und Art. 32 bei der Verarbeitung personenbezogener Daten durch geeignete technische und organisatorische Maßnahmen ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die staatlichen Stellen unterliegen ihrerseits gesetzlichen Bindungen zum Datenschutz, wenn sie personenbezogene Daten verarbeiten. Bei der Verarbeitung personenbezogener Daten zu Gefahrenabwehr- und Strafverfolgungszwecken durch die zuständigen Stellen findet auf Bundesebene u.a. das Bundesdatenschutzgesetz (BDSG), insbesondere dessen Teil 3, Anwendung. Durch die Regelungen in Teil 3 des BDSG sind die entsprechenden Vorgaben der Richtlinie (EU) 2016/680 (Datenschutz-Richtlinie) in Bundesrecht umgesetzt worden. Die Länder haben ihrerseits entsprechende Umsetzungsvorschriften erlassen bzw. bereiten deren Erlass vor. Nach § 47 Nr. 6 BDSG, der Art. 4 Abs. 1 Buchstabe f) der Datenschutz-Richtlinie umsetzt, müssen personenbezogene Daten in einer Weise erhoben und weiterverarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

§ 48 Abs. 2 BDSG, der Art. 29 der Datenschutz-Richtlinie umsetzt, sieht vor, dass bei der Verarbeitung besonderer Kategorien personenbezogener Daten geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen sind. Besondere Kategorien personenbezogener Daten sind gemäß § 46 Nr. 14 BDSG Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung. Geeignete Garantien können insbesondere spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle sein.

§ 71 BDSG regelt in Umsetzung des Art. 20 der Datenschutz-Richtlinie, dass der Verantwortliche u.a. in Bezug auf die Gestaltung und Nutzung von Datenverarbeitungssystemen angemessene Vorkehrungen zum Schutz personenbezogener Daten zu treffen hat (Abs. 1 Satz 1). Er hat hierbei unter anderem die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen (Abs. 1 Satz 2). Daneben hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist (Abs. 2 Satz 1). Dies betrifft insbesondere die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung und ihre Zugänglichkeit (Abs. 2 Satz 2). Die Maßnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können (Abs. 2 Satz 3). Damit wird die Anforderung formuliert, eine solche Zugänglichmachung stets durch menschliches Zutun einer Prüfung zu unterziehen. Abgesehen davon ist der Verantwortliche verpflichtet, nach den §§ 65 und 66 BDSG Verletzungen des Schutzes personenbezogener Daten dem Bundesdatenschutzbeauftragten und der betroffenen Person mitzuteilen. Mit diesen Vorschriften werden Art. 30 und Art. 31 der Datenschutz-Richtlinie umgesetzt. Diese Verpflichtung besteht bei Verletzungen der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten, die verarbeitet wurden, geführt haben, und kann in Bezug auf den Bundesdatenschutzbeauftragten nicht eingeschränkt werden.

Mit freundlichen Grüßen

Dr. Helmut Teichmann