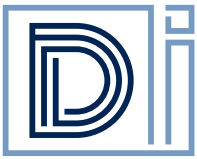

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Datenschutz und Informationsfreiheit

Dokumente 2016

Dokumente
zu Datenschutz
und Informationsfreiheit
2016

Impressum

Herausgeber: **Berliner Beauftragte für Datenschutz und Informationsfreiheit**
Friedrichstr. 219, 10969 Berlin
Telefon: (0 30) 1 38 89-0
Telefax: (0 30) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Druck: Druckerei Arnold

Stand: Januar 2017

Inhaltsverzeichnis

Vorwort

Die den Jahresbericht traditionell begleitende Sammlung von Dokumenten zu Datenschutz und Informationsfreiheit umfasst auch in diesem Jahr die Entschließungen der nationalen, europäischen und internationalen Datenschutzgremien sowie der Konferenz der Informationsfreiheitsbeauftragten in Deutschland. Diese Arbeitsergebnisse sind zugleich Zeugnis für das hohe Maß an Übereinstimmung, das zwischen den Beauftragten für Datenschutz und Informationsfreiheit sowohl national als auch europäisch und international vorherrscht. Das ist eine erfreuliche Feststellung und eine gute Grundlage für die künftige Arbeit der europäischen Aufsichtsbehörden, die vor dem Hintergrund der im Mai 2018 wirksam werdenden Europäischen Datenschutz-Grundverordnung immer enger zusammenarbeiten müssen.

Es ist daher nicht verwunderlich, dass die Dokumente dieses Bandes neben einer Vielzahl von aktuellen Entwicklungen schwerpunktmäßig die Auswirkungen dieser Grundverordnung auf die Arbeit und insbesondere die Zusammenarbeit der Aufsichtsbehörden behandeln.

Der Bogen der in den Dokumenten behandelten Themen spannt sich im Übrigen von vernetzten Kraftfahrzeugen und sogenannten Wearables bzw. Gesundheits-Apps über die Wahrung von Freiheits- und Persönlichkeitsrechten bei der Bekämpfung des internationalen Terrorismus bis hin zu Fragen des Datenschutzes im Bildungsbereich – ein Schwerpunktbereich in Zeiten sich rasant ausbreitender Digitalisierung. Im Bereich der Informationsfreiheit schließlich geht es um die Schaffung immer größerer Transparenz staatlichen Handelns.

Schon an den in diesem Band versammelten Materialien kann man erkennen, dass insbesondere die Fragen des Datenschutzes mittlerweile fast alle Lebensbereiche durchziehen und für alle Bürgerinnen und Bürger eine immer stärkere Bedeutung erlangen.

Maja Smoltczyk
Berliner Beauftragte für Datenschutz und Informationsfreiheit

A. Dokumente zum Datenschutz

I. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)

1. Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) vom 26. Januar 2016

Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge

Vorbemerkung

Bereits heute benötigt und produziert das moderne Kraftfahrzeug eine Vielzahl an Daten. Aufgrund der fortschreitenden informationstechnischen Ausstattung der Kraftfahrzeuge und deren Anbindung an das Internet sowie der Vernetzung der Verkehrsteilnehmer untereinander wird sich dieser Trend fortsetzen und in den kommenden Jahren zu weitreichenden Veränderungen im Straßenverkehr führen. Darüber hinaus entstehen zahlreiche neue Fahrzeugfunktionen und Verkehrstelematikanwendungen, z. B. in den Bereichen Service und Multimedia. Die Digitalisierung und insbesondere die Vernetzung bergen neben den unbestreitbaren Vorteilen für die Verkehrssicherheit und den Komfort zugleich auch Risiken für die Persönlichkeitsrechte der Fahrzeugnutzer. Vor diesem Hintergrund halten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder und der VDA nachfolgende datenschutzrechtliche Aspekte für besonders relevant[1].

1. **Personenbezogenheit:** Bei der Nutzung eines modernen Kraftfahrzeugs wird permanent eine Vielzahl von Informationen erzeugt und verarbeitet. Insbesondere bei Hinzuziehung weiterer Informationen können die anfallenden Daten auf den Halter oder auch auf den Fahrer und Mitfahrer zurückführbar sein und Informationen über persönliche oder sachliche Verhältnisse einer bestimmbaren Person enthalten. Die bei der Kfz-Nutzung anfallenden Daten sind jedenfalls dann personenbezogen im Sinne des Bundesdatenschutzgesetzes (BDSG), wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt.

[1] Datenschutzrechtliche Fragestellungen, die sich bei der Besitzüberlassung eines Kfz z. B. im Rahmen eines Dienst- oder Arbeitsverhältnisses oder einer Vermietung ergeben, sind nicht Gegenstand des vorliegenden Papiers.

2. Entscheidend ist der **Zeitpunkt der Datenerhebung** durch eine verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes. Hier ist zu unterscheiden, ob es sich um Kraftfahrzeuge handelt, bei denen eine Datenspeicherung innerhalb des Fahrzeuges stattfindet („offline"), oder ob eine Übermittlung von Daten aus dem Fahrzeug heraus erfolgt („online"), wie etwa bei der Übermittlung und Speicherung von Fahrzeugdaten auf Backend-Servern.

   Bei „Offline"-Autos ist von einer Datenspeicherung ohne vorherige Erhebung auszugehen. Eine Erhebung liegt mangels Erfüllung des Tatbestandes des § 3 Abs. 3 BDSG nicht vor; gleichwohl fallen anlässlich der Kfz-Nutzung Daten an, die im Fahrzeug abgelegt werden. Diese Daten müssen geschützt werden und machen – vergleichbar der Regelung in § 6c BDSG (Mobile personenbezogene Speicher- und Verarbeitungsmedien) – auch eine Sicherung des Rechts auf informationelle Selbstbestimmung erforderlich. Erst wenn die im Fahrzeug abgelegten Daten z. B. von einer Werkstatt für Reparaturzwecke ausgelesen werden, kommt es zu einer Erhebung durch eine verantwortliche Stelle nach § 3 Abs. 3 BDSG.

   Bei „Online"-Autos findet bereits im Zeitpunkt der Datenkommunikation aus dem Fahrzeug heraus eine Erhebung durch eine verantwortliche Stelle im Sinne des § 3 Abs. 3 BDSG statt.

3. **Verantwortliche Stelle**: Auch für die Identifikation der verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG ist zwischen „Offline"- und „Online"-Autos zu differenzieren.

   Bei „Offline"-Autos wird derjenige, der personenbezogene Fahrzeugdaten aus dem Fahrzeug ausliest (d. h. erhebt) und anschließend verarbeitet, zur verantwortlichen Stelle. Hierbei wird es sich in der Regel um Werkstätten handeln.

   Auch wenn die Hersteller bei „Offline"-Autos regelmäßig mangels Erhebung nicht bereits beim „Entstehen" der Daten verantwortliche Stelle sind, trifft diese unter anderem nach dem Gedanken „Privacy by Design" dennoch eine Verantwortung im Hinblick auf den Datenschutz. Dies gilt insbesondere, weil der Hersteller im Rahmen seiner technischen Gestaltungsmöglichkeiten (Art und Umfang von Schnittstellen, Zugriffsmöglichkeiten, Verfolgung der in § 3a BDSG niedergelegten Grundsätze von Datenvermeidung und -sparsamkeit) Einfluss auf die zeitlich nach hinten verlagerte Erhebung und Verarbeitung hat (vergleichbar der Regelung in § 6c BDSG). Sofern es um die technischen Gestaltungsmöglichkeiten geht, sind die Hersteller auch bei dieser Fahrzeugkategorie als Ansprechpartner für die Datenschutzaufsichtsbehörden anzusehen.

   Bei „Online"-Autos sind diejenigen als verantwortliche Stellen anzusehen, die personenbezogene Daten erhalten, d. h. in der Regel die Hersteller und gegebe-

nenfalls dritte Dienste-Anbieter. Insbesondere wenn Hersteller Zusatzdienstleistungen für das Kfz anbieten und dabei in ihren Backend-Servern Daten speichern, sind sie verantwortliche Stelle für diese Datenverarbeitung.

4. **Die Zulässigkeit der Datenerhebung und -verarbeitung** kann sich insbesondere aus § 28 Abs. 1 S. 1 Nrn. 1 oder 2 BDSG, §§ 11 ff. Telemediengesetz oder aus einer Einwilligung ergeben, die den Voraussetzungen des § 4 a BDSG genügt.

   Wie die Informationen über Datenerhebungs- und -verarbeitungsvorgänge aufbereitet sein müssen, um Teil des Vertrags oder Grundlage für eine ggf. relevante informierte Einwilligung sein zu können (ausführliche Informationen im Sinne eines Verfahrensverzeichnisses oder strukturierte, überblicksartige Informationen), bleibt Frage des Einzelfalls. Der Erstkäufer kann die notwendigen Informationen jedenfalls vom Verkäufer (Hersteller oder herstellergebundener Händler) erhalten.

   Grundsätzlich sind die wichtigsten Informationen zur Datenverarbeitung in allgemein verständlicher Form auch in der Borddokumentation nachlesbar vorzuhalten, die der Hersteller bereitstellt.

5. Gegenüber dem Hersteller besteht ein unentgeltliches **Auskunftsrecht** des Halters über seine durch den Hersteller erhobenen und gespeicherten personenbezogenen Daten nach § 34 BDSG. Darüber hinaus besteht aus § 34 BDSG kein datenschutzrechtliches Auskunftsrecht des Halters gegenüber dem Hersteller allein aufgrund dessen Gesamtverantwortung für die Gestaltung der datenspeichernden Systeme. Die Fahrzeughalter von „Offline"-Autos haben die Möglichkeit des Auslesens von Daten, ggf. mithilfe von Sachverständigen, was nicht zwingend unentgeltlich sein muss. Aufgrund des Transparenzgebots muss der Betroffene sich unentgeltlich und ohne sachverständige Hilfe über die Grundsätze der Datenverarbeitungsvorgänge einschließlich zumindest der Art der verarbeiteten personenbezogenen Daten beim Hersteller informieren können.

6. In Bezug auf die **Datenhoheit** sollen die Fahrzeugnutzer durch verschiedene Optionen über die Verarbeitung und Nutzung personenbezogener Daten selbst bestimmen können. Die Automobilhersteller streben an, durch standardisierte Symbole im Cockpit den aktuellen Vernetzungsstatus des Fahrzeugs erkennbar anzuzeigen und Möglichkeiten der jederzeitigen Aktivierung und Deaktivierung dieses Status' vorzusehen. Einschränkungen der Löschbarkeit bestehen bei rechtlichen Verpflichtungen oder dann, wenn entsprechende Daten im Zusammenhang mit Garantie- sowie Gewährleistungen oder der Produkthaftung von Bedeutung sind oder deren Verfügbarkeit für den sicheren Fahrzeugbetrieb erforderlich ist. Vom Nutzer eingegebene Informationen (z. B. Komfortdaten

wie Sitzeinstellung, bevorzugte Radiosender, Navigationsdaten, E-Mail-/SMS-Kontaktdaten, etc.) muss der Nutzer jederzeit selbst ändern oder zurückstellen können.

2. Entschließungen der 91. Konferenz vom 6./7. April 2016 in Schwerin

Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

Nach vier Jahren intensiver Diskussion ist der Text der Europäischen Datenschutz-Grundverordnung nun zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union abgestimmt. Mit der Grundverordnung verfügt die EU über ein weiterentwickeltes, einheitliches Datenschutzrecht, das für Unternehmen und Behörden in Deutschland weitgehend Kontinuität gewährleistet. Überall in Europa soll künftig dasselbe Schutzniveau für das Grundrecht auf Datenschutz gelten. Ebenso wird feststehen, dass sich auch außereuropäische Anbieter, die ihre Waren und Dienstleistungen auf dem europäischen Markt anbieten, an das europäische Datenschutzrecht halten müssen.

Wichtige datenschutzrechtliche Prinzipien wie der Grundsatz des Verbots mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz und der Grundsatz der Datensparsamkeit sind in den Verhandlungen weitgehend erhalten geblieben.

Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Abs. 11, 32 BDSG (Art. 88 i.V.m. Erwägungsgrund [EG] 155),

- Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4 i.V.m. EG 53, letzte beide Sätze),
- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Art. 58 und 83 Abs. 7 i.V.m. EG 150, vorletzter Satz),
- jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Art. 6 Abs. 2, 25, 32),
- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Art. 6 Abs. 4),
- Beibehaltung der Verpflichtung in § 4 f Abs. 1 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 4).

Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funk-

tionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können.

Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

- Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).
- Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.
- Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.
- Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.
- Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen.

Auch nach Brüssel gilt: Datenschutz verhindert nicht, Terroristen und ihre Helfernetzwerke zu erfassen und zu bekämpfen. Das geltende Datenschutzrecht erlaubt deren Daten zu speichern und Informationen wechselseitig auszutauschen. Der Datenschutz kann jedenfalls nicht für etwaige Defizite bei der Nutzung vorhandener Eingriffsbefugnisse sowie für möglicherweise ineffiziente sicherheitsbehördliche Strukturen verantwortlich gemacht werden.

Die häufig reflexartig erhobene Forderung nach weiteren Eingriffsbefugnissen und flächendeckenden Überwachungsmaßnahmen trägt zur Bekämpfung des internationalen Terrorismus nicht bei.

Es kennzeichnet den Rechtsstaat, dass sich jeder in einem fairen Verfahren gegen unberechtigte Verdachtsbehauptungen wehren, Schutz bei Gerichten suchen und auf die Kontrolle der Datenschutzbeauftragten vertrauen darf. Die massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht dem Grundrecht auf Datenschutz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell*, dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus sich daran messen lassen müssen, ob sie für dessen wirkungsvolle Bekämpfung wirklich geeignet, erforderlich und angemessen sind und damit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

*) – Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2001 in Münster

– Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg

– Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München

– Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

Datenschutz bei Servicekonten

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung so genannter Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Über diese Konten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Dabei soll der neue Personalausweis mit seiner eID-Funktion eine wichtige Rolle spielen. Eine Projektgruppe des IT-Planungsrates erarbeitet zurzeit die rechtlichen und technischen Rahmenbedingungen für Servicekonten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder nimmt die Aktivitäten des IT-Planungsrates zur Kenntnis, den Zugang zu elektronischen Verwaltungsdienstleistungen zu erleichtern und möglichst medienbruchfrei auszugestalten. Sie weist darauf hin, dass insbesondere die Einrichtung von länderübergreifenden Servicekonten gewichtige verfassungsrechtliche Fragen etwa zum Bund-Länder-Verhältnis und zum Persönlichkeitsrecht aufwerfen. So ist dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten. Servicekonten dürfen die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung nicht unterlaufen.

Hiervon abgesehen müssen jedenfalls die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz berücksichtigt werden. Für die Integration von Verwaltungsdienstleistungen heißt insbesondere, dass auch die Schnittstellen zwischen den Systemen so definiert sein müssen, dass nur die für den vorgesehenen Zweck erforderlichen Daten übertragen werden. Dazu sind folgende Rahmenbedingungen einzuhalten:

- Auch künftig muss es möglich sein, ohne Servicekonto Verwaltungsdienstleistungen in Anspruch zu nehmen.
- Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.
- Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogenen Daten als auch das Konto selbst löschen zu lassen.

- Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.
- Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default“ eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.
- Vorbehaltlich weiterer verfassungsrechtlicher Prüfungen ist für die Länder übergreifende Nutzung von Servicekonten eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle bzw. zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.
- Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nichtprivaten Zwecken bzw. zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.
- Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.

Sichere, elektronische Identifizierungsmöglichkeiten können zur Datenschutzkonformität von E-Government- und von E-Commerce-Verfahren beitragen. Die unabhängigen Datenschutzaufsichtsbehörden begrüßen daher Maßnahmen, die zur verstärkten Nutzung der eID-Funktion des neuen Personalausweises beitragen. Dennoch muss den Betroffenen die Möglichkeit gelassen werden, selbst zu

entscheiden, ob sie die eID-Funktion freischalten und nutzen wollen. Die Datenschutzkonferenz lehnt daher die angedachte Änderung des Personalausweisgesetzes ab, wonach die eID-Funktion des neuen Personalausweises dauerhaft eingeschaltet wäre und nicht mehr deaktiviert werden könnte. Eine standardmäßige Aktivierung der eID-Funktion wäre allenfalls dann hinnehmbar, wenn den Bürgerinnen und Bürgern ein Opt-In mit Widerrufsmöglichkeit angeboten wird, um die eID-Funktion jederzeit gebührenfrei aktivieren und deaktivieren zu können.

Orientierungshilfe[1] der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht (Stand: April 2016)

1. Zielsetzung

Immer mehr Bildungsinstitutionen setzen auf die webgestützte Wissensvermittlung und die elektronischen Kommunikationsmöglichkeiten zwischen Lehrenden und Lernenden. Zu diesen Zwecken werden auch an Schulen zunehmend Online-Lernplattformen für den Unterricht eingesetzt. Diese Online-Lernplattformen werden von Schulaufsichtsbehörden, Schulbuch-verlagen, Computer- und Softwareherstellern und sonstigen Anbietern bereitgestellt. Die Vorteile werden in der orts- und zeitunabhängigen Nutzung dieser Verfahren gesehen. Allerdings werden dabei zahlreiche Schüler[2]- und Lehrerdaten webbasiert verarbeitet. Die vorliegende Orientierungshilfe richtet sich insbesondere an Schulen, die Online-Lernplattformen als Lernmittel einsetzen wollen. Sie sollen sich einen Überblick darüber verschaffen können, welche datenschutzrechtlichen (Mindest-)Kriterien Online-Lernplattformen erfüllen müssen. Diese Orientierungshilfe gibt auch den Anbietern von Online-Lernplattformen die Möglichkeit, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine Nutzung durch Schulen zulässig ist.

Online-Lernplattformen sollen den Bildungs- und Erziehungsauftrag der Schule unterstützen, beispielsweise

- Kompetenzorientierung
- Integration fachlicher, methodischer und sozialer Lernziele
- Prozesshaftigkeit des Lerngeschehens
- Unterstützung von Schülern in Kleingruppen
- Begabungsgerechte Förderung

[1] beschlossen auf der 91. DSK am 6./7. April 2016 mit Gegenstimme des Bayrischen Landesbeauftragten für den Datenschutz

[2] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt eine adäquate weibliche Form gleichberechtigt ein.

- Erkennen individueller Lernfortschritte und Lernschwierigkeiten
- Beratung und Lernförderung einzelner Schüler

Ergänzend wird auf die Orientierungshilfe „Cloud Computing“ der Arbeitskreise Technik und Medien der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises in der aktuellen Fassung verwiesen, weil diese besondere Anforderungen für webbasierte Anwendungen bzw. „Datenverarbeitung in der Wolke“ aufzeigt.

Soweit die Online-Lernplattformen für andere als schulische Zwecke über das Internet zur Nutzung zur Verfügung stehen, gelten darüber hinaus die Vorschriften des Telemediengesetzes[3] und des Telekommunikationsgesetzes. Sie sind jedoch nicht Gegenstand dieser Orientierungshilfe.

2. Begriffsbestimmungen

Online-Lernplattformen im Sinne dieser Orientierungshilfe sind Softwaresysteme, die den Lehr- und Unterrichtsbetrieb durch die Bereitstellung und Organisation von Lerninhalten ergänzen oder sogar ersetzen. Schulsoftwaresysteme, die für Aufgaben der Schulverwaltung genutzt werden, sind davon systemtechnisch zu trennen.

Die virtuelle Lernumgebung einer Online-Lernplattform kann von der Schule so gestaltet werden, dass Kommunikation, Gruppenarbeit, Aufgabenbearbeitung und Lernkontrollen eingerichtet werden.

Leistungsbewertungen haben einen erhöhten Schutzbedarf. Dieser ist durch entsprechende technisch-organisatorische Maßnahmen abzusichern.

Der Zugriff auf die Software erfolgt ortsunabhängig mittels eines Endgerätes (PC, Tablet etc.) über einen Web-Browser. Die faktische Teilhabe der Schüler ist durch die Schule zu gewährleisten. Jeder Teilnehmer an einem bestimmten Kurs, also z. B. die Schüler einer Klasse oder eines Jahrgangs in einem bestimmten Schulfach, müssen sich vor einer Nutzung zunächst im Onlineverfahren auf der Lernplattform anmelden oder angemeldet werden. Das System stellt dann jedem Nutzer ein personalisiertes Benutzerkonto zur Verfügung. Darüber hinaus muss die Schule bzw. die verantwortliche Lehrkraft die Zugriffsrechte für die einzelnen Nutzer festlegen und die Funktionalitäten auswählen, die die Online-Lernplattform bietet (Bereitstellung von Lerninhalten, Diskussionsforen, Übungsaufgaben etc.).

[3] Die Ausnahme des § 11 Abs. 1 TMG greift in diesem Fall nicht.

3. Datenschutzrechtliche Problematik

In aller Regel melden sich die Benutzer solcher Plattformen personalisiert an und ihre Nutzungsbewegungen werden regelmäßig gespeichert. So wird beispielsweise festgehalten, welcher Nutzer wann auf welche Seite zugegriffen hat, sowie ob und mit welchem Ergebnis er sich an welchem Test beteiligt hat. Dadurch können Persönlichkeitsprofile über Schüler und Lehrkräfte erstellt werden.

Die schulrechtlichen Regelungen für die Verarbeitung und Nutzung von personenbezogenen Daten durch die Schule setzen voraus, dass die erhobenen Daten für die Aufgabenwahrnehmung durch die Schule erforderlich sein müssen. Viele Online-Lernplattformen stellen erheblich mehr Möglichkeiten zur Datenauswertung zur Verfügung, als dies für die Aufgabenwahrnehmung erforderlich ist und sind daher entsprechend anzupassen.

Auch beim Einsatz von Online-Lernplattformen benötigen Lehrkräfte die Möglichkeit, den Lernfortschritt einzelner Schüler zu beobachten, um im individuellen Beratungsgespräch oder bei der Planung und Umsetzung von lernförderlichen Interventionen gezielt den Schüler in seiner Lernsituation zu unterstützen. Weitergehende Angaben, z. B. wie oft und zu welchen Zeiten ein Schüler sich in der Online-Lernplattform an bestimmten Aufgaben beteiligt hat, dürfen in diesem Zusammenhang nicht eingesehen werden. Die Schüler und – falls erforderlich – auch die Erziehungsberechtigten sind vor der Nutzung der Online-Lernplattform darüber zu informieren, welche Auswertungsmöglichkeiten die Anwendung bietet und welche Konsequenzen das Nutzerverhalten haben kann.

Fazit:

- Die Online-Lernplattform ist so zu konfigurieren, dass ausschließlich die zur pädagogischen Aufgabenerfüllung der Schule erforderlichen Daten erhoben und verarbeitet werden.
- Es bietet sich die Nutzung von Online-Lernplattformen an, die je nach vorgesehenem Einsatzszenario modular angepasst werden können.
- Die Betroffenen sind vor der Nutzung der Online-Lernplattform über mögliche Auswertungen umfassend zu informieren.

4. Rechtsgrundlagen

Rechtsgrundlagen für die Verarbeitung personenbezogener Schülerdaten auch in Online-Lernplattformen sind zunächst die jeweiligen Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen. Ergänzend können – je nach Bundesland und Schultyp – die Landesdatenschutzgesetze sowie das Bundesdatenschutzgesetz zur Anwendung kommen.

Die verpflichtende Verwendung einer Lehrplattform kann nur durch oder aufgrund eines Gesetzes vorgeschrieben werden. Denkbar ist beispielsweise die Bestimmung als Lehrmittel durch entsprechende Verordnung. Andernfalls kann es nur auf Basis einer freiwillig erteilten Einwilligung[4] zum Einsatz einer derartigen Plattform kommen.

Fazit:

Vor dem Einsatz der Online-Lernplattform ist zu prüfen, ob deren Einsatz rechtlich zulässig ist und ob die Schüler und ggf. die Erziehungsberechtigten in die Nutzung der Plattform einwilligen müssen.

5. Verantwortliche Stelle

Bei der Nutzung von Lernplattformen bleibt die Schule – oder je nach Bundesland die Schulaufsichtsbehörde – verantwortliche Stelle für die Datenverarbeitung und -nutzung. Dies setzt voraus, dass sie die Art und Weise der Datennutzung und -verarbeitung maßgeblich bestimmen kann, also „Herrin der Daten“ bleibt. Lehrende dürfen im Rahmen der Freiheit der Gestaltung des Unterrichts nur insoweit Lernplattformen im Unterricht einsetzen, als die Schule oder die Schulaufsicht über den Einsatz der jeweiligen Lernplattform entschieden hat.

6. Umfang der Datenverarbeitung

6.1 Erforderliche Daten

Die Schule/Schulaufsichtsbehörde muss festlegen, welche Daten für die Nutzung der Online-Lernplattform zwingend benötigt werden.

6.1.1 Zwingend erforderliche Stammdaten

- Name und Anschrift der jeweiligen Schule und der verantwortlichen Stelle, die, wenn die Schulaufsichtsbehörde diese Aufgaben wahrnimmt, differieren können.
- Stammdaten zur Anlage von Benutzerkonten, die sowohl zur Identifikation des Nutzers im System als auch zum Zwecke der Vergabe von Rollen und Berechtigungen dienen. Es gibt die Möglichkeit, dass der Nutzer selbst die Daten eingibt und anlegt oder dass die Daten durch die Schule erfasst oder

[4] Es ist zu beachten, dass sich das Einwilligungserfordernis danach richtet, wie einsichtsfähig die Schüler sind. Die Erforderlichkeit der Einbeziehung der Eltern sollte mit dem zuständigen Landesbeauftragten für Datenschutz abgestimmt werden.

geändert werden. Wichtig ist, dass nur Daten eingegeben werden können, die für die sinnvolle Nutzung der pädagogischen Aufgabenerfüllung der Schule erforderlich sind.

- Bei der Benutzerverwaltung durch den Administrator ist zwischen dem Benutzernamen und dem Anmeldernamen zu unterscheiden. Der Benutzername muss den realen Namen (Klarname) des Benutzers enthalten. Der Klarname ist zur Identifikation des Schülers durch betreuende Lehrer erforderlich und muss nicht dem Anmeldenamen entsprechen. Der Anmeldename wird bei der Anmeldung im System verwendet und muss nicht mit dem Benutzernamen identisch sein. Im Gegenteil: die Nutzung von Pseudonymen als Anmeldenamen erhöht die Sicherheit im Vergleich zur Nutzung des Klarnamens. Der Anmeldename kann frei gewählt werden. Es wird die Anmeldung mit Pseudonymen empfohlen, um den Missbrauch des Kontos durch Dritte maßgeblich zu erschweren.
- Die Angabe einer E-Mail-Adresse ist je nach System optional oder zwingend erforderlich. Sie dient insbesondere der Zusendung von Benachrichtigungen aus den belegten Kursen sowie der Abfrage eines neuen Passworts bei dessen Verlust.

Ein Benutzerkonto kann weitere Informationen enthalten, die die Kommunikation innerhalb des Systems erleichtern, beispielsweise Klassenstufe, Bezeichnung der Lerngruppe, Ausbildungsgang (beispielsweise an berufsbildenden Schulen).

Fazit:

- Bei der Auswahl der Online-Lernplattform ist darauf zu achten, dass die Grundsätze der Datensparsamkeit und Datenvermeidung (z. B. nicht zu viele Stammdaten, Freitextfelder, Kommentarfunktionen) gewährleistet werden.
- Es ist eine pseudonymisierte Nutzerverwaltung der Lernplattform anzustreben.

6.1.2 Optionale Daten

Weitere optionale Daten können im Nutzerprofil auf freiwilliger Basis durch den Benutzer selbst erfasst werden. Bei missbräuchlicher Nutzung einzelner Informationen (beispielsweise im Zusammenhang mit Mobbing) sollten die betreffenden Felder für alle Benutzerkonten deaktiviert werden. Felder wie „Beschreibung“, „Nutzerbild“ und „Interessenfelder“ verdienen in diesem Zusammenhang besonderes Augenmerk.

Optionale Datenfelder können bei den gängigen Online-Lernplattformen sein:

- *Zeitzone:* Dieses Feld wird im Regelfall deaktiviert oder mit einem Standardwert belegt, da alle Nutzer in der Regel in der gleichen Zeitzone leben,
- *Beschreibung:* Hier können Nutzer Angaben zur eigenen Person eintragen. Diese sind innerhalb der Lernplattform, nicht aber öffentlich sichtbar. Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
- *Nutzerbild:* Der Nutzer kann eine Grafikdatei (beispielsweise ein Porträtfoto) hochladen, für die er die Urheberrechte besitzt. Dieses Feld ist nicht erforderlich, birgt die Gefahr von Rechtsverstößen und sollte deaktiviert werden.
- *Interessenfelder:* Hier können Schlagworte zur eigenen Person angegeben werden (beispielsweise Hobbys). Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
- *Webseite:* Teilnehmer können hier die URL zu einer eigenen Internetpräsenz angeben. Dieses Feld ist zu deaktivieren.
- *Bevorzugte Sprache:* Die Einstellung ermöglicht, dass Benutzeroberflächen in anderen Sprachen als Deutsch zur Verfügung stehen. Dieses Feld ist in aller Regel nicht erforderlich und sollte deaktiviert werden.
- *Institution, Abteilung:* Diese Information wird in der Regel in der Schule nicht verwandt.

Für organisatorische Zwecke können zusätzliche optionale Datenfelder angelegt und gepflegt werden. Dies ist nur zulässig, soweit es für die Aufgabenerfüllung erforderlich ist. Zu denken ist hier beispielsweise an die Angabe, an welchen Kursen ein Schüler teilnimmt, damit er Zugang zu den zugehörigen Dokumenten erhält. Nicht hierunter fallen persönliche Angaben wie Hobbies oder private Telefonnummern.

6.1.3 Nutzungsdaten

Bei der Nutzung einer Lernplattform werden automatisch Daten über den Nutzer und seine Aktivitäten erfasst und gespeichert. Diese Logdaten werden auf dem Server abgelegt, sie dürfen ausschließlich für die Überwachung der Funktionsfähigkeit und Sicherheit dieser Systeme sowie bei rechtswidrigem Missbrauch verwendet werden. Ergänzend wird auf die Orientierungshilfe „Protokollierung“ des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder in der aktuellen Fassung verwiesen. Näheres sollte in der Nutzungsordnung konkret festgelegt werden.

Nutzungsdaten sind in aller Regel für die Wahrnehmung schulischer Aufgaben nicht erforderlich und sollten daher nur unter klar definierten Voraussetzungen für

eindeutig bestimmte Personengruppen zu festgelegten Zwecken einsehbar sein. Nutzungsdaten sind beispielsweise

- Anmeldestatus: Erstlogin im System, letzter Login, Zeitpunkt der Abmeldung
- Protokollierung von Eingaben oder Änderungen
- IP-Adressen, genutzte Dienste (z. B. Dateidownloads, Chat)

6.1.4 Pädagogische Prozessdaten

Als pädagogische Prozessdaten werden Informationen bezeichnet, die dem Lehrer die Möglichkeit geben, den individuellen und kollektiven Lernprozess nachzuvollziehen, um didaktische Interventionen zu planen, Unterricht zu reflektieren, zu evaluieren und weiterzuentwickeln sowie individuelle Lernberatung für einzelne Schüler oder kleine Gruppen zu gestalten. In den verschiedenen Modulen einer Online-Lernplattform werden Prozessdaten generiert, die jeweils für unterschiedliche Personenkreise sichtbar sind. Solche Module sind:

- *Forendiskussion:* Die Beiträge können den Verfassern zugeordnet und in zeitlicher Struktur geordnet werden. Zudem zeigt die Darstellungsstruktur an, zu welchem Beitrag eine Antwort abgegeben wurde. Diese Informationen sind für alle Nutzer sichtbar. Eine Anzeige noch nicht gelesener Beiträge hingegen ist nur für den jeweiligen Einzelnutzer sichtbar.
- *Wiki-Einträge:* Ein Wiki ist ein mehrseitiges Dokument, an dem von verschiedenen Verfassern in einem Kurs gearbeitet wird. Durch die Speicherung der Historie ist erkennbar, wer welche Teile an einem Dokument bearbeitet hat. Die Lehrkraft kann dadurch die Beteiligung und die Beiträge Einzelner erkennen. Dies ist für Rückmeldungen und die Bewertung sowie die Förderung sozialer und kommunikativer Aspekte des Lernens wichtig.
- *Glossar (Datenbank):* Das Glossar stellt eine Sammlung von Informationen in strukturierter Form dar. Es enthält einzelne Texteinträge mit Angaben zum Erstellungszeitpunkt und dem Verfasser. Diese Details sind für alle Nutzer sichtbar.
- *Lernobjekte (Aufgaben, Tests):* Je nach Art des Objekts sind unterschiedliche Daten nur für Lehrkräfte oder auch für einzelne Schüler sichtbar. Eine Überwachung der außerunterrichtlichen Aktivitäten von Schülern durch Lehrende darf nicht stattfinden. Die Sichtbarkeit der Daten für Lehrende, ist pädagogisch zu begründen und von der Schulleitung bzw. der Schulkonferenz festzulegen.
- *SCORM-ModuIe, LTI-Module, Live Classroom, Plagiatsüberprüfung etc:* Bei der Nutzung derartiger Module werden unter Umständen personenbezogene

Daten an externe Dienstleister weitergegeben. Dies ist nur im Rahmen von bestehenden Auftragsdatenverarbeitungsverträgen zwischen Schule / Schulträger und Anbieter zulässig und ist datenschutzrechtlich gesondert zu prüfen. Prozessdaten von Lernenden dürfen nur dann für andere Teilnehmer sichtbar sein, wenn dies methodisch oder didaktisch erforderlich ist. Als Beispiel sei die Bewertungsfunktion in einem Diskussionsforum angeführt. Je nach Implementierung erlaubt sie eine schnelle, unter Umständen nonverbale Rückmeldung zu Beiträgen. Da auf diese Weise von Schülern auch unsachgemäße und verletzende Kritik gegenüber Mitschülern geäußert werden kann, ohne dass von Seiten der Lehrenden rechtzeitig eingegriffen werden kann, ist eine solche Funktion nur mit Bedacht zu aktivieren.

6.1.5 Statistische Daten

Die Lernplattformen erlauben die Auswertung statistischer Daten beispielsweise über Art und Umfang der Nutzung. Echte statistische Daten haben aber keinen Personenbezug und sind daher aus datenschutzrechtlicher Sicht unproblematisch. Sollte es sich nicht um echte statistische Daten in diesem Sinne handeln, gelten für sie die jeweiligen Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen der Länder.

6.2 Schriftliche Festlegungen

Vor dem Einsatz der Online-Lernplattform hat die Schule / die Schulaufsichtsbehörde schriftliche Festlegungen zur zulässigen Datennutzung und zum Rollen- und Berechtigungskonzept zu treffen. Außerdem muss dies in das Verfahrensverzeichnis aufgenommen werden.

Die Vorgaben zur Konfiguration und Anwendung der Online-Lernplattform durch die Administratoren, Lehrer und Lehrerinnen kann beispielsweise in Form einer Nutzerordnung geschehen, in der klar geregelt wird, wie die Vertraulichkeit, Integrität, Authentizität, die Nichtverkettbarkeit der Daten und die Intervenierbarkeit des Nutzers entsprechend dem jeweils geltenden Landesrecht vor Ort konkret umzusetzen ist. Hierzu gehören ein Löschkonzept (9.9) sowie die Frage, welche E-Mailadressen verwendet werden (9.2).

Fazit:

Die Grundlagen der Datenverarbeitungprozesse sind vor dem Einsatz der Online-Lernplattform abschließend in einer Nutzerordnung festzulegen.

7. Notwendige Prüfungen vor Inbetriebnahme

Vor dem Einsatz von Lernplattformen hat die verantwortliche Stelle (Schule oder Schulaufsichtsbehörde) im Zusammenwirken mit ihrem Datenschutzbeauftragten eine Vorabkontrolle nach den jeweils geltenden Landesregelungen durchzuführen. Hierbei sind insbesondere folgende Aspekte zu beachten:

- Einhaltung der ggf. bestehenden landesrechtlichen Regelungen zum Einsatz von Online-Lernplattformen

- Bei der Anschaffung einer Lernplattform eines externen Dienstleisters ist zu prüfen, ob dieser die datenschutzrechtlichen schulischen Anforderungen erfüllen kann.

- Gestaltung und Auswahl von Datenverarbeitungssystemen nach den Grundsätzen der Datenvermeidung und Datensparsamkeit

- Beim Einsatz von externen Dienstleistern sind die gesetzlichen Voraussetzungen der zulässigen Auftragsdatenverarbeitung zu beachten. Dabei gelten folgende allgemeine Anforderungen:
  - Die Schule/Schulaufsichtsbehörde muss „Herrin der Daten“ bleiben. Sie bestimmt, wer die Daten auf welche Weise verarbeitet und nutzt. Sie muss gegenüber dem Auftragnehmer ein Weisungsrecht in Bezug auf die Datenverarbeitung und -nutzung haben und sich vertraglich Kontrollrechte einräumen lassen.
  - Die Allgemeinen Geschäftsbedingungen externer Dienstleister sind unter Beachtung der hier dargestellten Grundsätze zu überprüfen und ggf. vertraglich abzuändern.
  - Mit dem Auftragnehmer ist ein Vertrag zu schließen, der den datenschutzrechtlichen Anforderungen an die Auftragsdatenverarbeitung genügt.

- Es gilt der Grundsatz der Zweckbindung. Danach ist insbesondere zu gewährleisten, dass die Daten der Schüler, Lehrer und Eltern nicht zu Werbezwecken genutzt werden.

- Die von der Schule/Schulaufsichtsbehörde zu erstellenden Nutzungsbedingungen, das Verfahrensverzeichnis und die sonstigen getroffenen technischen und organisatorischen Maßnahmen sind einer datenschutzrechtlichen Prüfung zu unterziehen.

8. Unterrichtungs-, Benachrichtigungs-, Schulungs- und Unterweisungspflichten

Schüler, Eltern[5] und Lehrkräfte sind vor dem Einsatz von Online-Lernplattformen ausführlich über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung ihrer Daten zu unterrichten. Sie sind darüber aufzuklären, dass sie jederzeit berechtigt sind, das Verfahrensverzeichnis der Lernplattform einzusehen. Sofern die Einwilligung für die Nutzung bestimmter Module erforderlich ist, sind sie ausdrücklich auf deren Freiwilligkeit und das bestehende Widerrufsrecht und dessen Rechtsfolgen zu informieren. Die Einwilligung ist schriftlich einzuholen. Aus der Einwilligung hat hervorzugehen, welche Daten, in welcher Form und zu welchem Zweck verarbeitet werden sollen. Darüber hinaus sind die Nutzer darüber zu informieren, ob und an wen Daten übermittelt werden.

Außerdem sind die Lehrkräfte und Administratoren entsprechend zu schulen und die Schüler entsprechend zu unterweisen.

9. Hinweise zur technischen und organisatorischen Umsetzung

9.1 Passwörter

Die Nutzung einer Online-Plattform erfordert einen passwortgeschützten Zugriff. Passwörter müssen verschlüsselt gespeichert werden. Es muss gewährleistet sein, dass niemand innerhalb der Lernplattform Passwörter im Klartext einsehen kann. Dies gilt auch für Administratoren.

Bei der Vergabe von Passwörtern durch die Schule ist zu gewährleisten, dass bei der ersten Nutzung des Logins der Nutzer sein Passwort ändern muss. Von dieser Regel kann im begründeten Einzelfall abgewichen werden (beispielsweise bei Grundschülern oder Schülern mit speziellem Förderbedarf). Nutzer mit der administrativen Berechtigung zur Bearbeitung der Benutzerkonten im System können für andere Nutzer Passwörter zurücksetzen. Von der Vergabe neuer Passwörter wird abgeraten, da dann der Administrator Kenntnis vom neuen Passwort erlangt. Bei der Passwortgenerierung, dem Passwortgebrauch und der Passwortverwaltung sollte die Maßnahme „M 2.11-Regelung des Passwortgebrauchs“ der vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten IT-Grundschutz-Kataloge beachtet werden. Dies betrifft insbesondere die Komplexität des Passwortes und die Geheimhaltungspflicht. Die Passwörter sind nach spätestens 90 Tagen gemäß M 2.11 zu wechseln.

[5] Hier ist zu beachten, dass die Eltern möglicherweise bei volljährigen Schülern nach dem geltenden Landesrecht nicht immer eine Zugriffsberechtigung haben dürfen.

Für die Verwendung von Passwörtern muss eine Vorgabe erfolgen, die die Mindestzahl an Zeichen und deren Zusammensetzung (Zahl der Großbuchstaben, Zahl der Kleinbuchstaben, Zahl der Ziffern und Zahl der Sonderzeichen) festlegt. Bei der Festlegung dieser Vorgaben ist das Alter der Schüler zu beachten, um keine Zugangsprobleme zu schaffen. Ein Passwort soll aber in keinem Falle kürzer als acht Zeichen sein.

9.2 E-Mail-Adresse

Die E-Mail-Adresse ist ein eindeutiger Wert. Soll eine E-Mail-Adresse innerhalb der Lernplattform zur Verfügung gestellt werden, dann ist sicherzustellen, dass diese E-Mail-Adresse nicht für mehrere Benutzerkonten verwendet werden kann. Die Verwendung der E-Mail-Adressen ist schriftlich zu regeln.

9.3 Erfassung der Daten des Benutzerkontos und Änderbarkeit

Benutzerkonten können durch Import, manuelle Eingabe oder Anbindung an eine bestehende Datenbank nach Maßgabe der in der Schule verwandten Systeme angelegt werden. Bei einem Import oder einer Anbindung an eine bestehende Datenbank sollte nur der Anmeldename, wie er im bestehenden Datenbestand gespeichert ist, an die Lernplattform übermittelt werden (unidirektionaler Informationsfluss). Dass Passwort muss den Richtlinien aus 9.1 entsprechen und daher evtl. neu vergeben werden. Die Schule oder die Schulaufsichtsbehörde legt die Vorgehensweise in Form von einer Nutzerordnung fest.

9.4 Öffentliche Bereiche

Es ist grundsätzlich möglich, bestimmte Bereiche einer Online-Lernplattform öffentlich zugänglich zu machen. Für diese Bereiche gelten dieselben datenschutzrechtlichen Regelungen wie für andere Internetpräsenzen von Schulen, insbesondere im Hinblick auf die Nennung von Namen oder die Abbildung von Schülern oder Lehrkräften; darüber hinaus gelten das Telemediengesetz und das Telekommunikationsgesetz. Unter Beachtung der einschlägigen Vorschriften muss eine allgemeine Zugänglichkeit immer unterbleiben, sobald dadurch personenbezogene Daten sichtbar werden.

9.5 Suchmaschinen

Bereiche, in denen nutzerspezifische Daten gespeichert werden, dürfen nicht öffentlich angeboten werden. Es ist dafür Sorge zu tragen, dass öffentliche Suchmaschinen (Google, Bing, etc.) keinen Zugriff auf diese Bereiche haben.

9.6 Rollenkonzept

Folgende Rollen sind in einer Online-Lernplattform in der Regel vorgegeben:

- *Administrator:* Der Administrator hat alle Berechtigungen für sämtliche Bereiche und Inhalte, er kann Benutzerkonten-Einstellungen ändern und systemweite Einstellungen vornehmen.
- *Kursverwalter:* Der Kursverwalter kann Bereiche anlegen und Berechtigungen vergeben. Das Recht kann auf Teilbereiche (Kurskategorien, beispielsweise Ausbildungsgänge, Fächer, Jahrgangsstufen) beschränkt werden.
- *Lehrkraft:* Die Lehrkraft kann in bestimmten Bereichen Inhalte pflegen, Teilnehmer zulassen, Lernfortschritte und Lernergebnisse einsehen.
- *Teilnehmer:* Teilnehmer können in den Bereichen arbeiten, zu denen sie eine Zugangsberechtigung haben, Lerninhalte nutzen und Eingaben tätigen.

In Übereinstimmung mit dem Rollen- und Berechtigungskonzept der Schule können weitere Rollen definiert werden.

Folgende Grundsätze sind bei der Vergabe von Rechten und Rollen zu beachten:

Ein **Administrator** kann auf alle Bereiche zugreifen. Personen mit Administrationsberechtigungen können daher alle Kurse sowie alle Beiträge der Schüler und Lehrer einsehen. Dies schließt Bewertungen mit ein. Bei der Vergabe von Administrationsrechten muss daher mit besonderer Sorgfalt vorgegangen werden und zwar:

- Jedem Administrator ist ein eigener personenbezogener Benutzeraccount zuzuweisen, d. h. es ist nicht zulässig, dass mehrere Administratoren das gleiche Benutzerkonto (= Gruppenadministratorkonto) nutzen. Der Anmeldename des Administrators muss pseudonym sein, um so eine missbräuchliche Kontosperrung zu verhindern. Das Pseudonym muss so gewählt werden, dass es nicht auf einfachem Weg herauszufinden ist.
- Administratoren, die gleichzeitig noch andere Tätigkeiten wahrnehmen, wie z. B. auch Lehraufgaben, müssen über ein separates Benutzerkonto für diese Zwecke verfügen. Es muss also die Möglichkeit bestehen, einer Person entsprechend ihrer verschiedenen Rollen mehrere Benutzerkonten zuweisen zu können.
- Die Anzahl der Administratorenkonten ist so gering wie möglich zu halten, um das Missbrauchsrisiko zu minimieren (z. B. unbefugte Kenntnisnahme, unkontrollierbare Rechtevergaben, etc.). Eine Vertretungsregelung muss aber gewährleistet sein.

- Administratorenrechte darf nur erhalten, wer innerhalb des Systems entsprechende Aufgaben tatsächlich wahrnehmen muss.
- Alle Aktivitäten der Administratoren sind ausschließlich zu Zwecken der Datenschutzkontrolle für einen Zeitraum von maximal einem Jahr zu protokollieren.

9.7 Zugriffsrechte

9.7.1 Zugriff durch schulinterne Stellen oder Personen

Welche Zugriffsrechte Lehrkräfte, die Schüler, die Schulleitung und der Administrator auf das System erhalten, ist in einem Rollen- und Berechtigungskonzept vorab schriftlich festzulegen. Dabei sind u. a. auch personalvertretungsrechtliche Vorgaben zu beachten.

Mitglieder der Schulleitung und gegebenenfalls Funktionsträger haben das Recht zur Durchführung von Unterrichtshospitationen. Dieses Recht dient der Wahrnehmung der Führungsaufgabe, der Beschaffung von Informationen und Eindrücken zur Unterrichts- und Schulkonzeptentwicklung. In vielen Schulen werden Klassenarbeiten exemplarisch nach der Bewertung und vor der Rückgabe an die Schüler der Schulleitung zur Information und Kenntnisnahme vorgelegt. Gleichwohl dürfen diese Zugriffe nur erfolgen, soweit es für die jeweilige Aufgabe erforderlich ist.

Werden Online-Lernplattformen eingesetzt, so werden sie automatisch zu einem Bestandteil der Unterrichtsarbeit. Damit gelten die schulinternen Vereinbarungen, die im Hinblick auf Hospitationen getroffen wurden, auch hier.

Die Art der Einsichtnahme der Schulleitung in die Arbeit mit einer Online-Lernplattform muss den schulinternen Vereinbarungen entsprechen, wie sie für Unterrichtshospitationen im Klassenraum gelten. Die Nutzer der Lernplattform sind über diese Vorgehensweisen und Vereinbarungen vor Beginn der Nutzung zu informieren. Jede Einsichtnahme wird in derselben Weise dokumentiert, wie dies für Hospitationen im regulären Unterrichtsbetrieb erforderlich und festgelegt ist.

Eine Überwachung der Arbeit mit der Lernplattform durch die Schulleitung oder andere Stellen und Personen ist nicht zulässig. Insbesondere darf auch eine Überwachung der Aktivitäten von Schülern durch Lehrende nicht stattfinden. Etwas anderes gilt, wenn die Plattform für pädagogische Aufgaben, wie organisierte Chats zu bestimmten Themen, Gruppenarbeiten usw. genutzt wird, die einer Benotung unterfallen. In diesem Fall darf die für die Benotung notwendig zu beobachtende Aktivität durch die Lehrkraft überwacht werden. Der Umfang der Daten, die für Lehrende sichtbar sein soll, ist daher pädagogisch zu begründen und von

der Schulkonferenz festzulegen. Ebenso wenig dürfen die Aktivitäten von Lehrenden durch Vorgesetzte auf der Online-Lernplattform überwacht werden. Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

9.7.2 Zugriff auf die Daten durch schulexterne Stellen oder Personen

Schulexterne haben grundsätzlich keinen Zugriff auf geschützte Bereiche der Online-Lernplattform. Sollte es in begründeten Ausnahmefällen nötig sein, so ist jeder Zugriff dieser Art zuvor durch die verantwortliche Stelle auf seine Rechtmäßigkeit zu prüfen. Die Teilnehmer sind über diesen Zugriff frühzeitig zu informieren. Es ist im Rahmen der datenschutzrechtlichen Vorschriften zulässig, externen Personen, die nicht als Lehrer, Schüler oder Mitarbeiter in der Schulverwaltung tätig sind, einen temporären und begrenzten Zugriff auch auf geschützte Bereiche der Lernplattform zu geben, sofern dies für die Gewährleistung der Funktion des Systems erforderlich ist, beispielsweise bei einer Fernwartung. Hierbei muss mit dem jeweiligen Auftragnehmer ein Vertrag über die Auftragsdatenverarbeitung abgeschlossen werden.

9.8 Datenlöschung

Soweit die Speicherung personenbezogener Daten einer Einwilligung bedarf, werden die gespeicherten Daten der Lehrer und Schüler gelöscht, wenn die Einwilligung widerrufen wird. Die Daten der Schüler in Kursen (letzte Bearbeitung, bearbeitete Lektionen, Fehler, Korrekturanmerkungen u. Ä.) werden jeweils am Ende des laufenden Schuljahres gelöscht. Aufbewahrungsfristen aus den Landesschulgesetzen bzw. zugehörigen Rechtsverordnungen sind ebenfalls zu beachten. Es ist schriftlich festzulegen, wie die Aufbewahrungsfristen eingehalten werden. Ausnahmen sind zulässig beispielsweise bei schuljahresübergreifenden Projekten zur Vorbereitung auf Nachprüfungen, bei abiturrelevanten Kursen und aufgrund von Dokumentationspflichten der Schule. Auch E-Portfolios der Schüler können im Sinne einer Sicherheitskopie während der Zeit des kompletten Schulbesuchs hinterlegt werden. Die übrigen Daten der Schüler und Lehrer werden spätestens am Ende des Schuljahres gelöscht, in dem die Lehrkraft von der Schule abgegangen ist oder der Schüler ausgetreten ist.

Benutzerkonten von Schülern und Lehrern sind nach deren Ausscheiden aus der Schule zu löschen oder wenn diese ihre Einwilligung widerrufen.

Die unter 6.1.3 genannten Log-Daten (z. B. wann welcher Nutzer auf welche Daten zugegriffen hat oder wann welche Funktionen genutzt wurden) fallen auf Serverseite an und ermöglichen es, Probleme beim technischen Betrieb und beim Zugriff der Nutzer im Bedarfsfall zu untersuchen und zu lösen. Die Speicherdauer sollte maximal zehn Tage betragen. Eine längere Speicherdauer ist

nur in begründeten Ausnahmefällen zulässig. Für weitergehende Regelungen zur Protokollierung wird auf die o. g. Orientierungshilfe „Protokollierung“ verwiesen.

Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

9.9 Trennung der Datenbanken

Jede Schule wird als eigenständige Organisationseinheit verstanden. Die Daten verschiedener Schulen sind logisch getrennt zu halten und zu verwalten. Es muss mindestens gewährleistet sein, dass Schulen nur auf ihre eigenen Daten zugreifen können. Hierzu wird auf die OH Mandantenfähigkeit des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in der jeweils aktuellen Fassung verwiesen.

9.10 Sonstige technische Maßnahmen

Es sollten konkrete Maßnahmen vorgeschlagen werden, die insbesondere den Zugriff externer Stellen auf die Daten verhindern und gewährleisten, dass die Datenübertragung auf den häuslichen Rechner der Lehrkräfte und Schüler sowie je nach Rollenkonzept ggf. der Eltern sicher vor unbefugtem Zugriff erfolgt. Die jeweils zu treffenden Maßnahmen richten sich dabei nach den konkreten Umständen des Einzelfalls. Je nach der Art der betroffenen Daten, dem Personenkreis, der auf sie Zugriff haben soll, dem Ort, an dem die Daten gespeichert werden, differiert das Maß der erforderlichen Sicherheit. Wenn es sich lediglich um eine reine Lernplattform handelt, die nur Informationen für die Schüler zur Verfügung stellt, sind nicht die gleichen hohen Schutzmaßnahmen erforderlich wie bei einer Plattform, auf der Noten abgespeichert werden und auf die in bestimmen Bereichen auch Dritte Zugriff haben.

Die Sicherheitsmaßnahmen betreffen insbesondere drei Punkte: die Datensicherheit auf dem Server, den Schutz des Administratorzugangs und den Schutz der Datenübertragung hin zum Nutzer.

1. Auf dem Server sollten nur Hintergrundsysteme zur Datenspeicherung eingesetzt werden, welche eine automatische Zugriffsrechteverwaltung mitbringen, die durch die Lernplattform auch genutzt werden sollte, d. h. ein Default-Nutzer als einziger Datenzugriffsberechtigter ist nicht zulässig (hier wäre sonst der Datenbestand unter Kenntnis des Default-Nutzers komplett auslesbar). Vor Einsatz einer entsprechenden Lernplattform muss das Programm dahingehend geprüft werden, dass eine voll umfängliche Nutzerverwaltung stattfindet.

2. Der Administratorzugriff ist innerhalb der Lernplattform ein sehr kritischer Punkt. Das Passwort sollte gängigen Sicherheitsvorkehrungen genügen. Es wird hierbei auf die jeweils aktuelle BSI Richtlinie zur Erstellung von Passwörtern verwiesen. In Anbetracht der sehr experimentierfreudigen Natur der Schüler sollte außerdem die Administration nur über für Schüler unzugängliche Rechner erfolgen, da dann ausgeschlossen werden kann, dass Schüler unbemerkt Schadsoftware installieren können, die dann das Administratorpasswort ausspähen könnte. Außerdem ist der Einsatz einer Firewall und aktueller Anti-Viren Software auf dem Server unerlässlich. Eine Zweifaktor-Authentisierung, wie sie bei vielen webbasierten Anwendungen Standard ist, wird für administrative Zugriffe bei Anwendungen mit erhöhtem Funktionsumfang (Tests, Hausaufgabenkontrolle, etc.) empfohlen.

3. Die Datenübertragung zwischen Server und Nutzer ist zu verschlüsseln. Je nach Lernplattform ist dabei der Einsatz der Verschlüsselungstechnologie einzeln zu prüfen.

3. Entschließung vom 20. April 2016

Klagerecht für Datenschutzbehörden – EU-Kommissionentscheidungen müssen gerichtlich überprüfbar sein

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert den Gesetzgeber auf, umgehend ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden vorzusehen. Wenn die unabhängigen Datenschutzbehörden der Auffassung sein sollten, dass eine Entscheidung der EU-Kommission rechtswidrig ist, wären sie gleichwohl an diese gebunden. Sie müssten daher ggf. gegen den rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung verstoßen. Um dies zu verhindern, sind die prozessualen Voraussetzungen dafür zu schaffen, dass die Datenschutzbehörden selbst bestehende Zweifel an der Rechtmäßigkeit einer Kommissionsentscheidung gerichtlich klären lassen können.

Anlass für die obige Aufforderung der Datenschutzkonferenz ist die zwischenzeitliche Vorlage einer Reihe von Dokumenten unterschiedlicher Repräsentanten der US-Administration durch die EU-Kommission am 29. Februar 2016, die für Unternehmen und Behörden Zusagen für den Umgang mit aus der EU übermittelten personenbezogenen Daten enthalten. Im Rahmen eines so genannten EU–US Privacy Shield sollen diese Dokumente Grundlage für eine künftige EU-Kommissionsentscheidung zur Angemessenheit des Datenschutzniveaus in den USA sein und damit als Nachfolgeregelung für die Safe Harbor-Entscheidung dienen. Letztere wurde bekanntlich am 6. Oktober 2015 durch den Europäischen Gerichtshof aufgehoben.

Gegen den „EU–US Privacy Shield“ bestehen jedoch nach Auffassung der Artikel-29-Datenschutzgruppe, dem Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten, erhebliche Bedenken. Die Artikel-29-Dateschutzgruppe hat zum „EU–US Privacy Shield“ zuletzt am 13. April 2016 detailliert Stellung genommen. Die Datenschutzkonferenz teilt diese umfassende Analyse und unterstützt die darin enthaltene Forderung an die EU-Kommission, vor einer Beschlussfassung substantielle Nachbesserungen vorzunehmen. Die Datenschutzkonferenz ist der Auffassung, dass auch der „EU–US Privacy Shield“ in seiner derzeitigen Form nicht ausreichend ist, das für die Übermittlung personenbezogener Daten in die USA erforderliche „angemessene Datenschutzniveau“ in den USA zu gewährleisten.

Der EuGH stellt in seiner o. g. Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klar, dass nach Maßgabe der Datenschutz-Richtlinie der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Zweifeln über eine Angemessenheitsentscheidung die Anrufung nationaler Gerichte ermöglichen, so dass diese den EuGH um eine Entscheidung über die Vereinbarkeit mit den europäischen Grundrechten ersuchen können.

Die Datenschutzkonferenz begrüßt und unterstützt daher ausdrücklich die Bundesratsinitiative der Freien und Hansestadt Hamburg zur zeitnahen Einräumung eines Klagerechts für die Datenschutzaufsichtsbehörden von Bund und Ländern (BR-Drs. 171/16), in der nochmals deutlich gemacht wird, „dass das vom Europäischen Gerichtshof (EuGH in seinem Urteil vom 6.10.2015 (Rechtssache C-362/14) statuierte Klagerecht für Datenschutzaufsichtsbehörden für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist“.

4. Entschließung[1] vom 25. Mai 2016

EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden

Am 14. April 2016 hat das Europäische Parlament dem neuen Rechtsrahmen für den Datenschutz in Europa zugestimmt. Wesentlicher Teil des Rechtsrahmens ist die EU-Datenschutz-Grundverordnung, deren Text am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde. Die Verordnung ist am 25. Mai 2016 in Kraft getreten und zwei Jahre später verbindlich in allen Mitgliedstaaten der Europäischen Union anzuwenden.

[1] Enthaltung Bayern (Bayerischer Landesbeauftragter für den Datenschutz und Bayerisches Landesamt für Datenschutzaufsicht)

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist darauf hin, dass mit der EU-Datenschutz-Grundverordnung eine Reihe neuer bzw. erweiterter Aufgaben auf sie zukommen. Hierzu gehören insbesondere:

- Bearbeitung von Beschwerden und Beratung Betroffener sowie datenschutzrechtliche Beratung und Kontrolle von Unternehmen nunmehr unter Beachtung des erweiterten räumlichen Anwendungsbereichs der Verordnung (Marktortprinzip),
- verpflichtende Beratung von Behörden und Unternehmen bei der Datenschutz-Folgenabschätzung, insbesondere im Rahmen der vorherigen Konsultation der Aufsichtsbehörde, sowie Beratung bei der Umsetzung neuer Anforderungen wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy By Design, Privacy By Default),
- Aufbau und Anwendung eines Kooperationsverfahrens zwischen Datenschutzbehörden in Europa bei grenzüberschreitenden Datenverarbeitungen (One-Stop-Shop), Verpflichtung zur gegenseitigen Amtshilfe und umfassender Austausch von Informationen zwischen federführenden und betroffenen Aufsichtsbehörden jeweils mit kurzen Bearbeitungsfristen,
- Etablierung eines Kohärenzverfahrens zwischen den Datenschutzbehörden in Europa zur Gewährleistung der europaweit einheitlichen Anwendung der Verordnung, Mitwirkung im Europäischen Datenschutzausschuss,
- europaweit einheitliche Auslegung der Grundverordnung in Bezug auf fehlende Regelungen (z. B. zur Videoüberwachung oder zum Scoring) und neue Anforderungen (z. B. Recht auf transparente Information oder Recht auf Datenübertragbarkeit),
- Erarbeitung von Stellungnahmen und Billigung von branchenspezifischen Verhaltensregeln zur ordnungsgemäßen Anwendung der Verordnung, Erarbeitung von Zertifizierungskriterien, ggf. Durchführung von Zertifizierungen, Erarbeitung von Kriterien für die Akkreditierung von Zertifizierungsstellen, ggf. Durchführung der Akkreditierung,
- Bearbeitung von gerichtlichen Rechtsbehelfen Betroffener gegen Entscheidungen von Aufsichtsbehörden,
- Ausübung neuer bzw. erweiterter Befugnisse der Datenschutzbehörden zur Erteilung von Anordnungen gegenüber den Verantwortlichen nunmehr auch im öffentlichen Bereich sowie Berücksichtigung zusätzlicher Tatbestände für Ordnungswidrigkeiten und eines erweiterten Bußgeldrahmens.

Die Europäische Datenschutz-Grundverordnung verpflichtet die Mitgliedstaaten, die Aufsichtsbehörden zur Gewährleistung ihrer Unabhängigkeit mit den er-

forderlichen personellen, finanziellen und technischen Ressourcen auszustatten (Art. 52 Abs. 4 DSGVO). Aus Sicht der Datenschutzkonferenz ist es für die Bewältigung der neuen Aufgaben zwingend erforderlich, für die Datenschutzbehörden in Deutschland erweiterte personelle und finanzielle Ressourcen vorzusehen. Dies gilt bereits für die jetzt laufende Vorbereitungsphase, in der die Weichen für eine funktionierende Umsetzung der Datenschutz-Grundverordnung gestellt werden. Die Konferenz appelliert deshalb an die Gesetzgeber in Bund und Ländern, rechtzeitig die haushaltsrechtlichen Vorkehrungen für eine jeweils angemessene, erweiterte Ausstattung der Datenschutzbehörden zu treffen. Nur so lassen sich die zusätzlichen Aufgaben der Datenschutz-Grundverordnung von den Datenschutzbehörden in Deutschland effektiv wahrnehmen.

5. Entschließungen der 92. Konferenz vom 9./10. November 2016 in Kühlungsborn

„Videoüberwachungsverbesserungsgesetz!“ zurückziehen!

Das Vorhaben des Bundesministeriums des Innern (BMI), durch ein „Videoüberwachungsverbesserungsgesetz“ Änderungen des Bundesdatenschutzgesetzes (BDSG) einzuführen, die künftig privaten Stellen den Betrieb von Videokameras zur Verhinderung von Anschlägen wie in Ansbach und Amokläufen wie in München erleichtern sollen, wird von den unabhängigen Datenschutzbehörden des Bundes und der Länder[1] abgelehnt. Der Gesetzentwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungenen Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es das Persönlichkeitsrecht in besonderem Maße zu schützen.

Gleichwohl lässt es die einschlägige Bestimmung des § 6 b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Abs. 3 Satz 2 BDSG können Videobilder an

[1] bei Enthaltung der Bundesbeauftragten für Datenschutz und Informationsfreiheit

Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben.

Terroristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen.

Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt. Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesinnenminister auf, den Gesetzentwurf zurückzuziehen.

Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf – Konsequenzen für polizeiliche Datenverarbeitung notwendig

Die Datenschutzbeauftragten des Bundes und der Länder[1] Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-West-

[1] bei Enthaltung Hamburgs

falen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte „Falldatei Rauschgift“ (FDR) datenschutzrechtlich geprüft.

Die FDR ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien aller Länder und die Zollfahndung haben Zugriff auf die Datei und können direkt Daten einspeichern und abrufen. Die Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

– Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Abs. 2 BKAG (Negativprognose) vorliegen.

– Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.

– Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.

– Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Absatz 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Ergebnisse machen deutlich:

1. Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.

2. Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.

3. In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert, nicht nur in der Falldatei Rauschgift die Mängel zu beheben. Vielmehr fordert sie die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizei. Erst recht ist dies erforderlich vor dem Einsatz der neuen Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV), die voraussichtlich im kommenden Jahr die FDR ablösen wird. Die Daten aus der FDR dürfen nicht pauschal übernommen werden.

6. Kühlungsborner Erklärung der unabhängigen Datenschutzbehörden der Länder[1] vom 10. November 2016

Der Vollzug der Europäischen Datenschutz-Grundverordnung (DS-GVO) erfordert eine effektive Organisationsstruktur. Zentrale Bedeutung kommt dabei dem Europäischen Datenschutzausschuss (EDSA) zu, der für alle Aufsichtsbehörden verbindliche Beschlüsse treffen kann und in dem jeder Mitgliedstaat eine Stimme hat.

Die Datenschutzbehörden der Länder fordern den Bundesgesetzgeber auf, bei der gesetzlichen Regelung des Vertreters der deutschen Aufsichtsbehörden im EDSA der Unabhängigkeit aller Aufsichtsbehörden und der Zuständigkeitsverteilung zwischen Bund und Ländern Rechnung zu tragen.

Der Vollzug der Datenschutzregelungen obliegt im föderativen System der Bundesrepublik Deutschland den Datenschutzbehörden der Länder. Die Zuständigkeit des/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) beschränkt sich auf wenige spezifische Bereiche. Diesem Umstand muss bei der Vertretung der deutschen Aufsichtsbehörden im EDSA nach Artikel 68 DS-GVO Rechnung getragen werden. Die unabhängigen Datenschutzbehörden der Länder setzen sich daher für die folgenden Regelungen ein:

- Die Vertretung der deutschen Aufsichtsbehörden im EDSA kann sowohl durch den/die BfDI als auch eine Landesaufsichtsbehörde erfolgen. Die Stellvertretung obliegt dann dem jeweils anderen.
- Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bestimmt die beiden Vertreter im EDSA.
- Die Vertretung im EDSA hat der nationalen Zuständigkeitsverteilung für den Vollzug Rechnung zu tragen. Die für den Vollzug zuständigen Aufsichtsbehörden müssen die Möglichkeit erhalten, über den Vertreter im EDSA Angelegen-

[1] bei Enthaltung Bayerns

heiten einzubringen und ihre jeweiligen Positionen im Verfahren autonom zu bestimmen.

Unter Zugrundelegung dieser Leitlinien ist nach Auffassung der Länder eine effektive Vertretung der unabhängigen Datenschutzbehörden im EDSA möglich.

II. Düsseldorfer Kreis – Oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

Beschluss vom 13./14. September 2016

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit („Kopplungsverbot“, Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),
- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung).

Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen (Stand: März 2016)

Diese Orientierungshilfe enthält Hinweise zur datenschutzgerechten Formulierung und Gestaltung von schriftlichen Einwilligungserklärungen nach § 4 a Bundesdatenschutzgesetz (BDSG) und elektronischen Texten nach § 13 Abs. 2 und Abs. 3 des Telemediengesetzes (TMG). Einwilligungen in Übermittlungen in Drittstaaten werden von dieser Orientierungshilfe nicht erfasst. Ergänzend sind gegebenenfalls die gesetzlichen Regelungen zu Allgemeinen Geschäftsbedingungen zu beachten.

In der täglichen Praxis der Datenschutzaufsichtsbehörden fällt immer wieder auf, dass in Antragsvordrucken von Firmen, Versicherungen, Banken, und anderen neben den vom Leistungsanbieter fest vorgegebenen Vertragsbedingungen die eventuell dazu ergänzend vorgesehenen datenschutzrechtlichen Einwilligungserklärungen nicht den Erfordernissen des § 4a BDSG entsprechen oder aber als „Einwilligungen" bezeichnete Texte vielmehr in Wirklichkeit als unabdingbare Vertragserklärungen bzw. allgemein geltende Geschäftsbedingungen einzustufen sind. Muss eine (AGB-rechtlich zulässige) Erklärung abgegeben bzw. Vertragsbedingung akzeptiert werden, um einen Vertrag abzuschließen, hat die betroffene Person also gar keine freie Wahlmöglichkeit, so handelt es sich nicht um eine datenschutzrechtliche Einwilligung nach § 4a BDSG, sondern um ein Vertragsangebot, das angenommen oder abgelehnt werden kann. Die mögliche Erlaubnis für den Datenumgang ergibt sich dann nicht aus § 4a BDSG, sondern aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG.

1. Überschriften

Bereits die Überschriften bringen häufig nicht klar genug zum Ausdruck, ob hier vom Antragsteller oder Kunden neben seiner hauptsächlichen Erklärung, beispielsweise dem Versicherungsantrag oder seiner Teilnahmeerklärung, noch zusätzlich eine datenschutzrechtliche Einwilligung abverlangt wird. Dies soll anhand einiger **Negativbeispiele** für Überschriften aufgezeigt werden:

- Datenschutzerklärung
- Datenschutz
- Datenschutzklausel
- Hinweis zum Datenschutz
- Erklärung zum Datenschutz
- Erklärung zur Datenverarbeitung

Im Gegensatz dazu weisen folgende dem § 4a BDSG entsprechende **Positivbeispiele** für Überschriften den Unterzeichnenden darauf hin, dass er mit Unterzeichnung eine datenschutzrechtliche Einwilligung abgibt:

- Einwilligungserklärung Datenschutz
- Datenschutzrechtliche Einwilligungserklärung
- Datenschutzrechtliche Einwilligungsklausel
- Einwilligungserklärung nach dem Bundesdatenschutzgesetz

2. Eindeutigkeit

Auch die Erklärung selbst ist zuweilen nicht eindeutig genug vorformuliert. So reicht es nicht aus, wenn sie mit den Worten beginnt: „*Mir ist bekannt, dass …*“. Hier ist dem Kunden nicht bewusst, dass er eine zusätzliche Erklärung abgibt.

Die notwendige Klarheit besteht nur, wenn die Formulierung den Erklärungscharakter eindeutig zum Ausdruck bringt, wie es in folgenden **Positivbeispielen** aufgezeigt wird:

- Ich willige ein, dass …
- Ich bin einverstanden, dass …
- Mit der Unterschrift geben Sie Ihre Einwilligung, dass …
- Durch Ihre Unterschrift wird die vorstehende Einwilligungserklärung mit den auf der Rückseite abgedruckten näheren Erläuterungen zur Datenverarbeitung und Datennutzung für …*(Zweck)* Bestandteil des Antrages.

Weiter muss es sich um eine bewusste Erklärung der betreffenden Person selbst handeln (opt-in). Schon von der verantwortlichen Stelle im Sinne einer Zustimmung vorangekreuzte Einwilligungstexte oder nur mit einer Streich-/Abwahl-Möglichkeit versehene „vorgegebene Zustimmungen“ (opt-out) genügen dem grundsätzlich nicht.

3. Freiwilligkeit

Eine wirksame datenschutzrechtliche Einwilligung im Sinne von § 4 a BDSG liegt nur dann vor, wenn diese freiwillig abgegeben werden und auch jederzeit widerrufen werden kann. Eine unter Druck oder Zwang abgegebene datenschutzrechtliche Einwilligung ist unwirksam.

4. Hervorhebung

In zahlreichen vorformulierten Einwilligungserklärungen fehlt es an der gemäß § 4 a Abs. 1 Satz 4 BDSG und – bei Einwilligung in Werbung – gemäß § 28 Abs. 3 a Satz 2 BDSG erforderlichen besonderen Hervorhebung gegenüber anderen Textpassagen, zum Beispiel durch

- Fettdruck, Schriftart oder Schriftgröße,
- farbliche Gestaltung der Schrift oder des Hintergrundes oder
- eine Umrahmung der Erklärung.

5. Platzierung

Die datenschutzrechtliche Einwilligungserklärung gehört als besondere beziehungsweise zusätzliche Willensäußerung der betroffenen Person in hervorgehobener Form (siehe unter Ziffer 4) grundsätzlich insgesamt auf das eigentliche Antragsformular und dort in aller Regel unmittelbar vor die Unterschrift, die dann sowohl die Hauptsacheerklärung (beispielsweise den Versicherungsantrag) als auch die datenschutzrechtliche Einwilligungserklärung abdeckt.

Denkbar ist aber auch bei längeren Einwilligungstexten eine besonders hervorzuhebende aussagekräftige Kurzfassung mit den wesentlichen Inhalten der datenschutzrechtlichen Einwilligungserklärung bei der Unterschrift mit einem Hinweis auf den beispielsweise auf der Rückseite oder auf einer Anlage enthaltenen erläuternden Text (siehe letztes Positivbeispiel unter Ziffer 2.).

Besonders datenschutzfreundlich – und in einzelnen Fallkonstellationen zwingend erforderlich (beispielsweise bei der beabsichtigten Übermittlung von Gesundheitsdaten) – ist es, wenn im Formular für die datenschutzrechtliche Einwilligung eine gesonderte Unterschrift vorgesehen ist.

Jedenfalls ist zur Sicherstellung der Eindeutigkeit und Freiwilligkeit (siehe Ziffern 2 und 3) erforderlich, dass die Einwilligungserklärung für ihre Gültigkeit ausdrücklich angenommen werden muss (beispielsweise durch ein Ankreuzen).

6. Trennung

In manchen Formularen werden die Datenschutzhinweise und -informationen nach § 4 Abs. 3 BDSG zu unabdingbaren Vertragsinhalten beziehungsweise allgemein geltenden Geschäftsbedingungen mit einer auf freiwilliger Basis abgefragten datenschutzrechtlichen Einwilligungserklärung nach § 4a BDSG vermischt. Unter der Überschrift „Datenschutzhinweise“ beginnt der Text mit Hinweisen und geht dann im weiteren Verlauf unvermittelt in eine Einwilligungserklärung über.

Dem Betroffenen wird hier nicht deutlich genug vor Augen geführt, dass er eine datenschutzrechtliche Einwilligungserklärung abgeben soll. Die reinen Informationen über Datenverarbeitung auf der Grundlage von Gesetz beziehungsweise Vertrag auf der einen Seite und die freiwillige datenschutzrechtliche Einwilligungserklärung auf der anderen Seite müssen textlich getrennt dargestellt werden. Eine mangelnde Trennung kann dazu führen, dass die Einwilligung als solche nicht erkannt wird und deshalb unwirksam sein kann.

7. Klare Zuordnung

Die ansonsten korrekt gestaltete datenschutzrechtliche Einwilligungserklärung soll nicht mit Datenverwendungen aufgebläht werden, die gar nicht einwilligungsbedürftig sind, da sie bereits auf Grund eines Gesetzes oder einer sonstigen Rechtsvorschrift zulässig sind.

Es ist vielmehr eine klare Zuordnung zur Einwilligung einerseits und zu den Datenschutzinformationen nach § 4 Abs. 3 BDSG andererseits vorzunehmen.

Ist es rechtlich strittig, ob eine Datenverwendung einer Einwilligung bedarf, bestehen keine Bedenken, sie unter Beachtung der oben genannten Formvorschriften „vorsichtshalber" in die Einwilligungserklärung mit einzubeziehen.

8. Einwilligung bei besonderen Arten personenbezogener Daten

Soweit sich die Einwilligung auf besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) beziehen soll, ist bei der formularmäßigen Gestaltung der Erklärung § 4 a Abs. 3 BDSG zu beachten, das heißt die Einwilligung muss ausdrücklich auch für diese besonderen Arten personenbezogener Daten erklärt werden.

9. Inhalt von Einwilligungen

Der Text der Einwilligungserklärung muss die betroffene Person klar und allgemein verständlich über die zu verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die verantwortliche Stelle informieren, und muss, soweit nach den Umständen des Einzelfalls erforderlich, auf eventuelle Folgen der Verweigerung der Einwilligung hinweisen (§ 4 a Abs. 1 Satz 2 BDSG).

Auf die grundsätzlich gegebene Widerrufsmöglichkeit der Einwilligung ist hinzuweisen; im Bereich der Telemedien ist ein solcher Hinweis durch § 13 Abs. 3 TMG sogar ausdrücklich vorgeschrieben (siehe bei Nr. 10).

Wenn im Rahmen der Verarbeitung auch Datenübermittlungen an Dritte in Betracht kommen, sind die Datenübermittlungen mit deren Zweckbestimmung und die Empfänger der Daten transparent zu erläutern.

Eine undifferenzierte, nicht mehr überschaubare Darstellung einer großen Anzahl genannter Datenempfänger kann den Transparenzanforderungen widersprechen und nach der zivilrechtlichen Rechtsprechung zu einer Unwirksamkeit der Einwilligung führen.

10. Einwilligung bei Telemedienangeboten

Wird eine Einwilligung elektronisch im Rahmen eines Telemedienangebotes eingeholt (beispielsweise auf einer Webseite), so sind gemäß § 13 Abs. 2 und Abs. 3 TMG einige Besonderheiten zu beachten:

Danach muss der Diensteanbieter sicherstellen, dass

- der Nutzer die Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen und
- mit Wirkung für die Zukunft widerrufen kann.

Der Nutzer muss zudem vor Erklärung der Einwilligung auf sein jederzeitiges Widerrufsrecht hingewiesen werden, wobei diese Information für den Nutzer jederzeit abrufbar sein muss. Diese Unterrichtung kann beispielsweise in der Datenschutzerklärung erfolgen.

11. Werbeeinwilligungen

Hierzu wird auf die ergänzenden Regelungen in § 28 Abs. 3 a und 3 b BDSG hingewiesen. Siehe insoweit auch die Ziffern 2 und 4 der Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke, https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Anwendungs-hinweise_Werbung.pdf.

III. Europäische Konferenz der Datenschutzbeauftragten

Budapest, 26./27. Mai 2016

Entschließung zu neuen Kooperationsrahmen

– Übersetzung –

Präambel

Das wichtigste Unterfangen der europäischen Datenschutzbeauftragten in den letzten Jahren war es, zur Überarbeitung des bisherigen europäischen Datenschutzrechtsrahmens beizutragen. Dazu gehört insbesondere die Verabschiedung der EU-Datenschutzgrundverordnung und die EU-Richtlinie für den Datenschutz in Polizei und Justiz sowie die Aktualisierung der Europarats-Konvention 108.

Am 17. Dezember 2015 einigten sich die europäischen Gesetzgeber auf ein neues EU-Datenschutzpaket, welches 2016 förmlich verabschiedet wurde. Es sieht vor, dass nach einer zweijährigen Vorbereitungsphase ein neues Datenschutzsystem in Kraft tritt, in dem die Mitgliedstaaten enger zusammenarbeiten und koordiniert handeln. Dabei bleiben die bestehenden zentralen Datenschutz-Grundsätze größtenteils unverändert.

Das neue Datenschutzsystem legt strengere Verpflichtungen und Auflagen für verantwortliche Stellen und Auftragsdatenverarbeiter fest und entwickelt das Verhältnis zwischen den Datenschutzbehörden und die Regeln ihrer Zusammenarbeit weiter. Wenn die neue EU-Datenschutz-Grundverordnung im Jahr 2018 wirksam wird, müssen die europäischen Datenschutzbehörden gut vorbereitet sein.

Die europäischen Datenschutzbehörden haben bereits auf verschiedenen Ebenen Erfahrungen mit grenzübergreifenden Mechanismen gesammelt, unter anderem im Rahmen der Artikel-29-Datenschutzgruppe, in dem Europarat und den Case-Handling Workshops der europäischen Frühlingskonferenz. Ebenfalls erprobt ist die Zusammenarbeit auf der Ebene der internationalen Datenschutzkonferenz, die Instrumente und Mittel zur grenzüberschreitenden Zusammenarbeit entwickelt und dazu eine jährliche Konferenz ins Leben gerufen hat.

Die Europäische Konferenz der Datenschutzbehörden weist darauf hin,

– dass der Rechtsrahmen des Datenschutzes in Europa sich grundlegend verändert hat und dieser Prozess von den Datenschutzbehörden dynamisches und

proaktives Handeln erfordert, um sich auf kohärente Zusammenarbeit und Rechtsdurchsetzung vorzubereiten;

– dass die EU-Datenschutz-Grundverordnung als unmittelbar anwendbares Recht zu wesentlichen Veränderungen in allen EU-Mitgliedsstaaten führen wird;

– dass der Anwendungsbereich der EU-Datenschutz-Grundverordnung weiter gefasst ist als das bisherige Recht, was den Datenschutzbehörden neue Aufgaben und Befugnisse bringt. Das Gleiche trifft auch auf die modernisierte Konvention 108 zu;

– dass Datenschutzbehörden unter der neuen EU-Datenschutz-Grundverordnung verpflichtet sind, ihre Aufgaben und Pflichten EU-weit kohärent umzusetzen;

– dass parallel die bereits existierende Zusammenarbeit mit Verbraucherschutzinstitutionen verfestigt und Synergien zwischen Verbraucher-, Kartell- und Datenschutzrecht identifiziert und genutzt werden sollten, insbesondere im Bereich der digitalen Gesellschaft und der digitalen Wirtschaft;

– dass die Zusammenarbeit der Datenschutzbehörden in grenzüberschreitenden Fällen nicht nur wichtig, sondern der einzige effektive und effiziente Weg ist, um die Rechte der Betroffenen durchzusetzen;

– dass es die zentrale Aufgabe der Datenschutzbehörden darstellt, das Recht auf Privatsphäre und Datenschutz als Grundrecht im Sinne der Grundrechtscharta der Europäischen Union zu wahren;

– dass die Datenschutzbehörden in der zweijährigen Vorbereitungszeit bis zum Inkrafttreten der Verordnung eng miteinander und allen Beteiligten zusammenarbeiten müssen, etwa mit den Regierungen, nationalen Parlamenten, den öffentlichen und privaten Sektoren sowie der Wissenschaft;

– dass für die Förderung der Zusammenarbeit zur internationalen Durchsetzung von Regelungen auf Erfahrungen zurückgegriffen werden sollte, etwa aus der Arbeit in der Artikel-29-Datenschutzgruppe, den Frühlingskonferenz-Case-Handling-Workshops und den neueren von der internationalen Datenschutzkonferenz aktivierten Ressourcen.

Die Konferenz

1. betont, wie wichtig es ist, die Grundrechte der Betroffenen effektiv zu schützen;

2. fordert die europäischen Datenschutzbehörden zu einer engeren, mehr Eigeninitiative zeigenden und effektiveren Kooperation auf;

3. erinnert die europäischen Datenschutzbehörden an die Notwendigkeit eines pragmatischen und innovativen Ansatzes, insbesondere eines verstärkten Dialogs und Informationsaustauschs mit anderen Kontrollinstanzen, die dafür zuständig sind, die Rechte und Interessen des Einzelnen in der digitalen Gesellschaft und Wirtschaft zu wahren;

4. ermutigt die europäischen Datenschutzbehörden, mit ihren nationalen Regierungen zu verhandeln, um die nötigen personellen und finanziellen Ressourcen sicherzustellen, die sie für die neuen Aufgaben und Verpflichtungen benötigen;

5. empfiehlt, dass auf künftigen Frühlingskonferenzen über die Erfolge bei der Zusammenarbeit und gemeinsamen Anstrengungen berichtet wird.

Entschließung zu grenzüberschreitenden Transfers personenbezogener Daten

– Übersetzung –

Präambel

In den vergangenen Jahrzehnten hat die Bedeutung personenbezogener Daten für die Zivilgesellschaft und die digitale Wirtschaft weltweit zugenommen. Die Zahl der privaten und öffentlichen Datenverarbeiter nimmt weiter zu. Hintergrund sind zahlreiche Innovationen und neue Technologien, die es ermöglichen, dass ständig personenbezogene Daten grenzüberschreitend fließen und Stellen auf der ganzen Welt Zugang zu diesen Daten haben.

Die neueren Entwicklungen bei der grenzüberschreitenden Übertragung personenbezogener Daten haben dazu beigetragen, die Kommunikationsbarrieren zwischen verantwortlichen Stellen und Auftragsdatenverarbeitern, die sich nicht im gleichen Land befinden, zu überwinden. Das hat die globalen kulturellen, ökonomischen und öffentlichen Beziehungen gestärkt. In diesem Kontext sollte berücksichtigt werden, dass der Bereich der grenzüberschreitenden personenbezogenen Datenflüsse die Interessen der gesamten Gesellschaft berühren kann.

Um dabei den effektiven Schutz persönlicher Daten zu gewährleisten und die inhärenten Risiken grenzüberschreitender Datenflüsse aufzufangen, müssen die gesetzlichen Rahmenbedingungen geschaffen werden, die ausreichende Sicherheitsmaßnahmen zum Schutz der Grundrechte und Grundfreiheiten des Individuums vorsehen.

Das Recht auf Schutz der personenbezogenen Daten ist ein Grundrecht. Datenschutzbehörden spielen eine wichtige Rolle beim Schutz der Rechte des Individuums und bei der Schaffung öffentlichen Bewusstseins für diese Rechte, insbesondere wenn es um grenzüberschreitende Datenflüsse geht.

Hinweise der europäischen Konferenz der Datenschutzbehörden

– Das Recht auf Datenschutz geht auf Artikel 8 der Charta der Grundrechte der Europäischen Union zurück. Es hat damit den Rang eines Grundrechts im EU-Recht. Das bedeutet, dass dieses Recht von EU-Institutionen und Mitgliedsstaaten bei ihrer Interpretation des EU-Rechts zu beachten und zu garantieren ist.

– Die OECD-Datenschutzrichtlinien (2013) weisen darauf hin, dass der anhaltende grenzüberschreitende Fluss personenbezogener Daten hohe internationale Datenschutzstandards sowie eine verstärkte Kooperation der Datenschutzbehörden noch notwendiger machen.

– Wie im Entwurf der überarbeiteten Konvention 108 bestätigt, verlangt das Zusatzprotokoll der Konvention des Europarats ein angemessenes Schutzniveau, wenn persönliche Daten in Länder übertragen werden, die nicht Mitglied der Konvention sind. Betroffene in Europaratskonvention-108-Vertragsstaaten sollten einheitliche Garantien zum Schutz ihrer Rechte erhalten. Zudem sollen für die Veröffentlichung oder das Zugänglichmachen von Daten an einen Empfänger in einem Drittstaat, der nicht dem Recht der Konventions-Mitgliedstaaten unterliegt, einheitliche Garantien gelten.

– Der Europäische Gerichtshof hat am 6. Oktober 2015 im Fall „Maximilian Schrems gegen den Datenschutzbeauftragten“ entschieden, die „Safe-Harbor-Entscheidung“ aufzuheben und die Befugnisse der unabhängigen Datenschutzbehörden wie in Artikel 28 der Direktive 95/46 vorgesehen zu stärken.

– Der Europäische Gerichtshof hat festgelegt, dass Drittstaaten ein „im wesentlichen äquivalentes“ Datenschutzniveau vorweisen müssen, wenn personenbezogene Daten auf Grundlage eines Angemessenheitsbeschlusses übermittelt werden sollen.

– Wenn in dem Drittland kein angemessenes Schutzniveau vorliegt, muss die verantwortliche Stelle in Übereinstimmung mit der Richtlinie 95/46/EG im Einzelfall adäquate Sicherheitsmaßnahmen für diese Übermittlung vorweisen. Die Frage der Übermittlung personenbezogener Daten aus Europa ist untrennbar mit der Notwendigkeit verknüpft, sicherzustellen, dass europäische Standards außerhalb von Europa eingehalten werden, insbesondere wenn es um den Zugang zu Daten sowie deren Nutzung und Veröffentlichung durch Dritte geht.

Die Konferenz

1. appelliert an die europäischen Datenschutzbehörden, das Bewusstsein der Betroffenen für ihre Rechte in Bezug auf grenzüberschreitende Datentransfers zu fördern, etwa das Auskunftsrecht sowie mögliche Rechtsmittel und Sanktionen.

2. ermutigt die europäischen Datenschutzbehörden, ihre wesentliche Aufgabe der effektiven Durchsetzung von Datenschutzregeln zu erfüllen und sich zusammenzutun, um angesichts der jüngsten rechtlichen Entwicklungen zu grenzüberschreitenden Datenflüssen Probleme in der Praxis zu identifizieren.

3. betont die große Bedeutung des „EU–US-Privacy Shields“, das die aufgehobene „Safe Harbor“-Entscheidung ersetzen soll. Die Konferenz begrüßt die bedeutenden Verbesserungen des Privacy Shields im Vergleich zu „Safe Harbor“, stärkt das Vorhaben der Europäischen Kommission, an weiteren Klarstellungen und Verbesserungen zu arbeiten, und verpflichtet sich, den weiteren Verlauf von Gesetzgebungsverfahren in diesem Bereich genau zu überwachen.

4. erinnert an die Bedeutung enger Zusammenarbeit und des Erfahrungsaustauschs, insbesondere beim Monitoring der technologischen Entwicklungen im Zusammenhang mit grenzüberschreitenden Datenflüssen.

IV. Internationale Konferenz der Datenschutzbeauftragten

38. Konferenz, 17.–20. Oktober 2016, Marrakesch[1]

Entschließung über die Annahme eines internationalen Kompetenzrahmens für die Datenschutzerziehung

– nichtamtliche Übersetzung –

Die 38. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre:

Verweist auf die internationalen Abkommen, insbesondere in Bezug auf die Rechte der Kinder:

– Die Genfer Erklärung über die Rechte des Kindes vom 26. September 1924;

– Das Übereinkommen der Vereinten Nationen über die Rechte des Kindes vom 20. November 1989;

Unter Hinweis auf die internationalen Empfehlungen im Zusammenhang mit der Erziehung von Kindern und Jugendlichen, nämlich:

– Die Empfehlung Rec(2006)12 des Ministerkomitees des Europarats an die Mitgliedstaaten betreffend die Befähigung von Kindern für die neue Informations- und Kommunikationsumgebung vom 27. September 2016;

– Die Erklärung des Ministerkomitees des Europarates über den Schutz der Würde, der Sicherheit und der Privatsphäre von Kindern im Internet vom 20. Februar 2008;

– Die OECD-Empfehlung des Rates zum Schutz der Kinder im Online-Umfeld vom 16. Februar 2012;

– Die Entschließung der UNESCO über Internet-Fragen, einschließlich des Zugangs zu Informationen und Wissen sowie die freie Meinungsäußerung, der Privatsphäre und der ethischen Dimension der Informationsgesellschaft, angenommen auf der 37. Tagung im November 2013;

[1] Bei den nachfolgenden Entschließungen handelt es sich um keine offiziellen amtlichen Übersetzungen. Es kann daher keine Gewähr für die korrekte Wiedergabe des Inhalts übernommen werden.

Unter Hinweis auf internationale Erklärungen, die Staaten ermuntern, bei ihren mittel- und langfristigen Anstrengungen, eine hochwertige Bildung zu fördern und Bildung für alle, einschließlich der digitalen Erziehung, als Priorität zu setzen:

– Die 2015 angenommene Incheon-Erklärung der UNESCO, die die Bildung 2030 definiert: *Inklusive und chancengerechte hochwertige Bildung sowie lebenslanges Lernen für alle*, ein Aktionsrahmen zur Förderung, insbesondere, globaler staatsbürgerlicher Bildung durch Rückgriff auf Informations- und Kommunikationstechnologien (IKT);

Unter Hinweis auf die beiden Entschließungen der 30. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre im Jahr 2008:

– Entschließung zum Datenschutz in sozialen Netzwerkdiensten;

– Entschließung zum Schutz der Privatsphäre von Kindern im Internet, die die Datenschutzbeauftragten zur Entwicklung von Programmen für die digitale Erziehung auffordert, insbesondere für junge Menschen;

Unter Verweis auf die Entschließung der 35. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre über die digitale Bildung für alle aus dem Jahr 2013, in der empfohlen wird, dass die Datenschutzbeauftragten:

– Die Datenschutzerziehung in Programmen zur digitalen Kompetenz fördern

– An der Ausbildung von Multiplikatoren teilnehmen, und zwar durch das Organisieren von oder Mitarbeit an der „Ausbildung von Ausbildern“ im Bereich des Datenschutzes;

In dem Bewusstsein, dass in vielen Staaten die digitale Erziehung für Kinder im schulpflichtigen Alter heutzutage, auf nationaler oder sub-nationaler Regierungsebene, als Handlungsschwerpunkt gilt;

In der Erkenntnis, dass nach den Rechtsordnungen der Mitglieder die auf Schulen ausgerichtete Bildungspolitik auf verschiedenen Regierungsebenen beruht, und dass Datenschutzvorschriften von Land zu Land unterschiedlich sind, und dass diese Entschließung unter diesen Umständen immer noch sinnvoll sein kann;

In der Erwägung, dass es für die effektive Ausstattung mit Kenntnissen für die aktive Teilnahme an der heutigen digitalen Gesellschaft und der digitalen Wirtschaft wichtig ist, bereits bei Schulbeginn bei den Kindern das Bewusstsein über die Auswirkungen der Nutzung und Weitergabe von Daten zu wecken, auch auf einer gemeinsamen Basis von konkreten und operationellen Fähigkeiten in Bezug auf den Datenschutz; und dass in diesem Zusammenhang die Hervorhebung von da-

tenschutzrechtlichen Fragen als Teil der Erziehung zur digitalen Kompetenz, die auf die nationalen Bedingungen zugeschnitten ist, ein wesentlicher Bestandteil der Herausbildung von Staatsbürgern und der Achtung der Menschenrechte ist;

In der Erkenntnis, dass trotz der Qualität der in Bezug auf den Datenschutz entwickelten pädagogischen Ressourcen ein Mangel an Ausbildung für Erzieher hinsichtlich des Datenschutzes besteht, mit Ausnahme einiger weniger Länder;

Darauf hinweisend, dass die Ausbildung von Lehrkräften Auswirkungen auf die Erziehung der Schüler hat und dass die Schulen die Mittel haben müssen, um den Bürgern die verantwortungsvolle und ethische Nutzung der neuen Technologien beizubringen;

In der Erwägung, dass in Zusammenarbeit mit Bildungsfachleuten, Regierungsvertretern und anderen betroffenen Interessengruppen die Datenschutzbehörden aufgrund ihres Fachwissens einen nützlichen Beitrag zu dieser Ausbildung leisten können;

Feststellend, dass es in diesem Zusammenhang notwendig ist, eine gemeinsame Basis konkreter und operabler Fähigkeiten in einem internationalen Kompetenzrahmen zur Erziehung der Schüler zum Datenschutz vorzuschlagen.

Die auf der 38. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre anwesenden Behörden sehen die Empfehlung der folgenden Maßnahmen als eine wichtige Priorität an:

- Die Aufnahme der Datenschutzerziehung in Studienprogrammen und Lernplänen;
- Die Schulung von Lehrkräften im Bereich des Datenschutzes, damit sie notwendigen Sachverstand sowie praktische Erfahrungen in diesem Bereich erhalten und dadurch in die Lage versetzt werden, jungen Menschen zu helfen, kritisches Denken zu entwickeln, was die Nutzung personenbezogener Daten betrifft;
- In diesem Sinne die Einführung gezielter Schulungsmaßnahmen, die sich sowohl auf die Vorteile als auch auf die Risiken bei der Verwendung neuer Technologien beziehen, und auch auf Verfahren, die es uns ermöglichen, ein Leben in einem digitalen Umfeld mit Zuversicht, Klarheit und Achtung der individuellen Rechte zu führen.

Infolgedessen werden die Behörden Folgendes unternehmen:

1. Die Verabschiedung des internationalen Kompetenzrahmens für die Datenschutzerziehung von Schülern […]. Des Weiteren werden sie Regierungen und

insbesondere die für die Bildung zuständigen Behörden sowie sonstige Interessengruppen, die im Bildungsbereich arbeiten, auf die Bedeutung folgender Aspekte aufmerksam machen:

– Die Förderung der Nutzung und der praktischen Entwicklung des Kompetenzrahmens in Zusammenarbeit mit den Datenschutzbehörden im Rahmen von Studienprogrammen und Lehrplänen, sowie die Ausbildung von Lehrkräften, und zwar unabhängig von den unterrichteten Fächern;
– Die Förderung der Forschung in Pädagogik und Didaktik in Bezug auf den Datenschutz, so dass die Entwicklung von Aktivitäten und Ressourcen in diesem Bereich sich auf wissenschaftliche Studien und Berufserfahrung stützen.

2. Der Internationalen Arbeitsgruppe für digitale Bildung folgende Aufträge erteilen:

– Sicherzustellen, dass Datenschutzbehörden, in Zusammenarbeit mit ihren nationalen Behörden und relevanten Interessengruppen, die Gewinnung von pädagogischen Ressourcen, die auf die in diesem Rahmen angesprochenen Kompetenzen und auf die betreffende Altersgruppe zugeschnitten sind, vorschlagen oder dazu beitragen können;
– Die Gewährleistung einer Nachverfolgung der Fortschritte bei der Entwicklung der Kompetenzen im Bereich des Datenschutzes in Bezug auf die digitale Erziehung in Bildungsprogrammen.

Die U.S. Federal Trade Commission enthält sich der Abstimmung, da die Entschließung einen einheitlichen internationalen Rechtsrahmen annimmt, ohne anzuerkennen, dass sich mit anderen Ansätzen, die die Vielfalt der weltweit existierenden Rechtsvorschriften zum Datenschutz und der kulturellen Werte widerspiegeln, ebenfalls das gemeinsame Ziel der Förderung der digitalen Erziehung erreichen ließe.

Entschließung zur Entwicklung neuer Messgrößen für die Datenschutzregulierung

– nichtamtliche Übersetzung –

Die 38. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre:

Unter Berücksichtigung, dass:

a) Im Jahr 2013 die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung beobachtet hat, dass „die aktuell im Bereich des Datenschutzes verfügbare Beweisgrundlage unausgewogen ist“[1]:

b) Ausgehend von dieser Einsicht die OECD den Ländern empfohlen hat, „die Entwicklung international vergleichbarer Messgrößen für die politische Entscheidungsfindung in Bezug auf den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr personenbezogener Daten zu fördern“[2]:

c) Im Jahr 2016 die Minister der OECD die Absicht zur engen Zusammenarbeit mit allen Interessengruppen erklärten, um Erfahrungen auszutauschen und gemeinsam an einem „Beitrag zur Entwicklung neuer Messgrößen für die digitale Wirtschaft, wie etwa für Vertrauen, Fähigkeiten und globale Datenströme“[3] zu arbeiten:

d) Die Möglichkeit der Messung häufig als eine Voraussetzung für die wirksame Steuerung und Verbesserung angesehen wird:

e) Der Auftrag der Konferenz Wissen zu verbreiten und praktische Hilfe zur wirksamen Unterstützung der Behörden bei der Wahrnehmung ihrer Aufträge zu leisten“ durch die Schließung der Lücken der im Datenschutzrecht vorhandenen Maßnahmen vorangebracht werden wird:

Beschließt die Konferenz daher:

1. Sich bei der Hilfe zur Entwicklung international vergleichbarer Messgrößen in Bezug auf den Datenschutz einzubringen sowie die Bemühungen anderer internationaler Partner nach Fortschritten in diesem Bereich zu unterstützen:
2. Das Exekutivkomitee anzuweisen, nach Möglichkeiten zu suchen, wie die Konferenz die Entwicklung international vergleichbarer Messgrößen fördern kann:
3. Als erster Schritt wird das Exekutivkomitee ermächtigt, Verfahren einzuführen:
   a) Zur Aufforderung der Mitgliedsbehörden, bestimmte gemeinsame zentrale Fragen in ihren regelmäßigen Meinungsumfragen aufzunehmen, die beispielsweise den Grad der Sensibilisierung der DSBs und der geltenden Datenschutzgesetze ansprechen;
   b) Zum zentralen Empfang der Ergebnisse; zu ihrer Bereitstellung und zur Berechnung von Richtwerten

[1] OECD, Begründung zu den überarbeiteten OECD Richtlinien (2013)

[2] OECD-Rat über Leitlinien für den Schutz der Vertraulichkeit und für den grenzüberschreitenden Austausch personenbezogener Daten (2013), Art. 22

[3] Die Ministererklärung der OECD Über die digitale Wirtschaft (Die Erklärung von Cancun), Juni 2016

4. Dem Exekutivkomitee die Genehmigung zur Einberufung von Arbeitsgruppen zu erteilen, die ihn bei der Aufgabe unterstützen, sofern dies nötig ist.

ERLÄUTERUNG

Die moderne öffentliche Politik strebt die Verfolgung eines rationellen wissenschaftlichen Ansatzes an, wo immer dies möglich ist. Ein Aspekt dabei ist das Bestreben, Dinge zu messen. Die Messung gilt als nützlich für das Verständnis der bestehenden Situation, wie sie sich gegenüber der Vergangenheit geändert hat, und vorherzusagen, wie sie sich in der Zukunft ändern könnte. Messungen sind auch bei der Definition des Problems nützlich und bei der Bewertung der Auswirkungen von staatlichen Interventionen.

Beispielsweise könnte es nützlich sein, Aspekte der Datenschutzlage in der Vergangenheit zu quantifizieren, das Ergebnis mit dem gegenwärtigen zu vergleichen und die verschiedenen Änderungen oder Entwicklungen mit entsprechender Belastbarkeit zu bewerten. Im Idealfall könnte die Wirkung der Datenschutzvorschriften oder der Erfolg verschiedener Interventionen, wie zum Beispiel die Meldepflicht für Datenschutzverletzungen, bewertet werden.

Die OECD hat ein besonderes Interesse an der Messbarkeit sowohl von datenschutzrechtlichen Regelungen als auch der Wirtschaft. Die OECD stellte erhebliche Lücken in den verfügbaren statistischen Daten fest, die als Grundlage für politische Entscheidungen zum Datenschutz dienen. Die OECD fordert die Entwicklung international vergleichbarer Messgrößen als Informationen für den politischen Entscheidungsfindungsprozess in Bezug auf den Schutz der Privatsphäre.

Datenschutzbehörden können am stärksten von vergleichbaren Messgrößen profitieren, die entwickelt werden könnten. DSBs könnten sehr wahrscheinlich auch Quellen für Daten sein, die bei der Entwicklung solcher Messgrößen dienlich sein könnten. Die Konferenz vereint mehr als 110 Behörden aus der ganzen Welt und sieht daher einen besonderen Wert bei der Entwicklung nützlicher Messgrößen für den Datenschutz.

Diese Entschließung spiegelt die Bedeutung dieses Themas wieder und würdigt die Absicht der OECD, in diesem Bereich eine Führungsrolle zu übernehmen. Die OECD hat zweifellos ein erhebliches statistisches Fachwissen. Die Konferenz ist bereit, sich bei der Entwicklung international vergleichbarer Messgrößen in Bezug auf den Datenschutz einzubringen.

Als kleinen ersten Schritt schlägt die Entschließung die Schaffung eines Konferenzverfahrens vor, das Behörden zur Aufnahme bestimmter gemeinsamer

zentraler Fragen in ihren regelmäßigen Meinungsumfragen anregen soll. Dieser Vorschlag stützt sich auf die Erfolge bei der staatenübergreifenden Abstimmung einer Umfragen zu den Entwicklungen des überarbeiteten EU-Datenschutzgesetzes (durch eine spezielle „Eurobarometer"-Umfrage[4]). Das Forum der asiatisch-pazifischen Datenschutzbehörden(APPA) empfahl außerdem die Annahme gemeinsamer Kernfragen für Meinungsumfragen, und das wurde als Modell für diesen Aspekt der Entschließung verwendet[5].

Die Entwicklung international vergleichbarer datenschutzrechtlicher Fragen bei Meinungsumfragen wird als ein einfacher Ausgangspunkt für einen sinnvollen Beitrag der Konferenz im Hinblick auf die Herausforderung bei der Entwicklung nützlicher und international vergleichbarer Messgrößen für den Datenschutz gesehen. Die DSBs könnten sich zukünftig anderen schwierigen Bereichen zuwenden, für die sie bereits die administrativen Daten haben, wie in den Bereichen der Beschwerden, Untersuchungen, strategische Beratungen, Durchsetzung mit dem Ziel der Ableitung nützlicher internationaler Messgrößen.

Die Entschließung schlägt vor, dass das Exekutivkomitee sich einige vorbereitende Arbeiten vornimmt, um erfolgsversprechende Wege zu ermitteln, die man weiterverfolgen sollte. Bei Bedarf kann eine Arbeitsgruppe zur Unterstützung eingerichtet werden.

Entschließung zu Menschenrechtsverteidigern

– nichtamtliche Übersetzung –

38. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre:

Verweist auf Folgendes:

(a) Jeder Mensch hat das Recht, als Einzelner wie auch in Gemeinschaft mit anderen, ohne Unterscheidung jeglicher Art, etwa nach Rasse, Hautfarbe, Geschlecht, Sprache, Religion, politischer oder sonstiger Anschauung, nationaler oder sozialer Herkunft, Vermögen, Geburt oder dem sonstigen Status, den Schutz und die Verwirklichung der Menschenrechte und Grundfreiheiten auf nationaler, regionaler und internationaler Ebene zu fördern und darauf hinzuwirken:

[4] Eurobarometer Spezial 431, Datenschutz: http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm

[5] APPA Forum, Erklärung über gemeinsame Verwaltungspraktiken hinsichtlich empfohlener gemeinsamer Kernfragen für Erhebungen zu den Meinungen der Gemeinschaft, Juni 2014: http://www.appaforum.org/resources/common_practice.html#surveys

(b) Die Sicherstellung, dass die gebührende Achtung, der Schutz und die Verwirklichung des Rechts auf Privatsphäre und auf den Schutz personenbezogener Daten eine gemeinsame Verantwortung ist, die nicht ausschließlich den Datenschutzbehörden überlassen bleiben kann, sondern der Aufmerksamkeit und Handlungsbereitschaft vieler Akteure innerhalb der Regierung, der Wirtschaft und Zivilgesellschaft bedarf:

(c) Die Generalversammlung der Vereinten Nationen verabschiedete 1999 die Erklärung über das Recht und die Pflichten von Einzelpersonen, Gruppen und gesellschaftlichen Organen, allgemein anerkannte Menschenrechte und Grundfreiheiten zu fördern und zu schützen (besser bekannt unter der Bezeichnung der Erklärung über die Menschenrechtsverteidiger):[1]

(d) Der Sonderberichterstatter für die Lage der Menschenrechtsverteidiger hat festgestellt, dass die Erklärung noch nicht hinreichend bekannt ist und dass weitere Anstrengungen erforderlich sind, um für ein besseres Verständnis seitens der Regierungen bezüglich ihrer Pflichten zu sorgen:

(e) Auf einzelstaatlicher Ebene in den meisten Ländern, und in zunehmendem Maße auch auf globaler Ebene, gibt es Verfechter und Aktivisten für den Schutz der Privatsphäre und der Daten, die als „Menschenrechtsverteidiger" bezeichnet würden (schlichtweg Personen, die als Einzelne wie auch in Gemeinschaft mit anderen für die Förderung oder den Schutz von Menschenrechten eintreten):

(f) Die Einrichtung unabhängiger nationaler Institutionen zur Förderung und zum Schutz der Menschenrechte und Grundfreiheiten durch Staaten, unabhängig davon, ob es sich um Ombudspersonen, Menschenrechtskommissionen oder jede andere Form der nationalen Einrichtungen handelt, nimmt zu und sollte unterstützt werden:[2]

(g) Der Menschenrechtsrat der Vereinten Nationen verabschiedete im Jahr 2016 die Resolution für die Förderung, den Schutz und den Genuss der Menschenrechte im Internet, die unter anderem;[3]

a. alle Menschenrechtsverletzungen und Übergriffe gegen Personen aufgrund der Wahrnehmung ihrer Menschenrechte und Grundfreiheiten im Internet verurteilt, und sie fordert alle Mitgliedstaaten in diesem Zusammenhang auf, für die Rechenschaftsplicht zu sorgen; und

[1] In mehreren Sprachen verfügbar unter: http://tinvurl.com/HRDefenders.

[2] Siehe Grundsätze betreffend die Stellung nationaler Institutionen (Pariser Grundsätze), http://tinvurl.com/paris-principles.

[3] Verfügbar in allen Amtssprachen der VN auf: http://tinvurl.com/humanightsinternet.

b. Maßnahmen zur absichtlichen Verhinderung oder Unterbrechung – unter Verletzung internationaler Menschenrechte – des Zugangs zu Informationen und ihrer Verbreitung im Internet verurteilt, und sie fordert alle Staaten auf, solche Maßnahmen zu unterlassen und einzustellen:

(h) Gewalttaten und anderen Übergriffe auf Menschenrechtsverteidiger können die wesentliche Rolle beeinträchtigen, die Menschenrechtsverteidiger in der Gesellschaft spielen, und lassen alle Personen, für die sie kämpfen, wehrlos zurück:

(i) Unternehmen sind verpflichtet, dafür Sorge zu tragen, dass ihre Handlungen nicht zu Menschenrechtsverletzungen oder zur Behinderung legitimer friedlicher Aktivitäten von Menschenrechtsverteidigern beitragen:[4]

Daher beschließt die Konferenz:

1. Die Anerkennung der Arbeit von Menschenrechtsverteidigern als wichtig für den Aufbau einer soliden und nachhaltigen demokratischen Gesellschaft, und der wichtigen Rolle der Menschenrechtsverteidiger im Prozess der vollständigen Verwirklichung der Rechtsstaatlichkeit und der Stärkung der Demokratie:

2. Die Förderung eines stärkeren Bewusstseins hinsichtlich der Erklärung über die Menschenrechtsverteidiger:

3. Die Aufforderung an die Regierungen zur Stärkung der Wirksamkeit der Erklärung im Inland:

4. Die Fortsetzung der Förderung von Transparenz und von unabhängiger Aufsicht in den Bereichen der staatlichen Überwachung zur Unterstützung demokratischer Institutionen und einer informierten Zivilgesellschaft:

5. Die Ermutigung der Regierungen zur Bereitstellung und Förderung sicherer und wirksamer Kanäle für Einzelpersonen, damit sie schlechte Praktiken im Bereich des Datenschutzes melden, um Abhilfe für Verletzung der Datenschutzvorschriften verlangen zu können, oder um gegen unverhältnismäßiges Vorgehen gegen die Rechte auf den Schutz der Privatsphäre und der Daten vorzugehen:

6. Die Anerkennung, dass unabhängige und mit ausreichend Befugnissen ausgestattete Datenschutzbehörden für den Schutz der Menschenrechtsverteidiger unerlässlich sind.

[4] Siehe die Website Leitprinzip der VN für Unternehmen und Menschenrechte (2011) https//:tinyurl.com/hrbusinessprinciples und die Arbeit des Sonderbeauftragten der Vereinten Nationen für die Frage der Menschenrechte und transnationaler Unternehmen sowie anderer Wirtschaftsunternehmen http://tinvurl.com/SRHRbusiness.

7. Die Unterstützung der Bemühungen des Menschenrechtsrats der Vereinten Nationen und des Sonderberichterstatters der Vereinten Nationen für das Recht auf Privatheit in Bezug auf die Förderung, den Schutz und den Genuss der Menschenrechte, insbesondere im Internet:

8. Die Förderung der Zusammenarbeit zwischen den Datenschutzbehörden und internationalen, regionalen und nationalen Menschenrechtsinstitutionen:[5]

9. Sich zu verpflichten, auf künftigen Konferenzen die datenschutzrechtlichen Fragen, die die Menschenrechtsverteidiger betreffen, weiter zu erörtern.

ERLÄUTERUNG

Datenschützer und Aktivisten sind ein wesentlicher Bestandteil einer aufgeklärten und aktiven Zivilgesellschaft. Diese Personen können beispielsweise unter der Bevölkerung Informationen über Rechte in Bezug auf den Datenschutz und den Schutz der Privatsphäre verbreiten. Sie bringen Fälle von Datenschutzverletzungen vor Datenschutzbehörden oder vor Gerichte und können bei Gesetzgebern Petitionen zur Reform von Gesetzen einreichen, oder sie können gegen Eingriffe und Praktiken von Seiten des Staates oder von Unternehmen protestieren. In der Terminologie im Bereich der Menschenrechte sind diese Personen als „Menschenrechtsverteidiger“ bekannt.

Die Vereinten Nationen haben eine Erklärung über die Menschenrechtsverteidiger verabschiedet, die durch Leitlinien des Hohen Kommissars der Vereinten Nationen für Menschenrechte[6] und von dem Sonderberichterstatter der Vereinten Nationen für die Lage von Menschenrechtsverteidigern[7] weiter ausgearbeitet wurde. Auch andere regionale Gruppierungen haben Hinweise erteilt.[8]

Die Erklärung der Vereinten Nationen und damit zusammenhängende Leitlinien sollen den Wert der Arbeit von Menschenrechtsverteidigern entsprechend anerkennen und sie schützen. Die Entschließung der Konferenz will mit dem Aufbau auf der vorherigen Arbeit im Bereich der Menschenrechte beginnen, insbesondere im Zusammenhang mit dem Schutz der Privatsphäre und dem Datenschutz.

---

[5] Auf internationaler Ebene sind in humanitären Hilfsorganisationen arbeitende Menschenrechtsverteidiger Risiken ausgesetzt. In der Erläuterung zu der Entschließung über den Schutz der Privatsphäre und humanitäres Handeln, angenommen auf der 37. Konferenz, wird angemerkt, dass humanitäre Organisationen, die keine Privilegien und Immunitäten genießen, unter den Druck geraten können, für humanitäre Zwecke erhobene Daten an Behörden zu übermitteln, die diese Daten für andere Zwecke verwenden wollen (z. B. zur Kontrolle der Migrationsströme und zur Terrorismusbekämpfung). Das Risiko des Datenmissbrauchs könnte gravierende Auswirkungen auf die Datenschutzrechte von Vertriebenen haben und kann zu einer Beeinträchtigung ihrer Sicherheit sowie generell für humanitäre Maßnahmen führen.

[6] Siehe z. B. http://tinyurl.com/UNHCRHRdefenders.

[7] Siehe z. B. http://tinyurl.com/OHCHRHRDCommentary.

[8] Siehe z. B. http://tinyurl.com/EUHRDguidelines und http://tinyurl.com/COEHRdefenders.

Die Entschließung betont auch die Rolle der verschiedenen Interessengruppen und Institutionen. Sie hebt die Verantwortung für die Achtung der Menschenrechte seitens der Unternehmen und Regierungen hervor. Die Entschließung ermutigt die Datenschutzbehörden zur Zusammenarbeit mit nationalen Menschenrechtsinstitutionen, um Menschenrechtsverteidiger zu fördern und zu schützen.

Hinweis: In der Entschließung über spezifische Datenschutz- und Sicherheitsrisiken wurden Risiken ermittelt, einschließlich des Potenzials für die Entwicklung von Überwachungssystemen, die durch Technologien, wie Management-Informationssysteme, elektronische Übermittlungen, digitale Identitätsfeststellung, Mobiltelefone, und auch durch Drohnen, erhöht werden können. Humanitäre Organisationen, die keine Privilegien und Immunitäten genießen, könnten unter den Druck geraten, für humanitäre Zwecke erhobene Daten an Behörden zu übermitteln, die diese Daten für andere Zwecke verwenden wollen (z. B. zur Kontrolle der Migrationsströme und zur Terrorismusbekämpfung). Das Risiko des Datenmissbrauchs könnte gravierende Auswirkungen auf die Datenschutzrechte von Vertriebenen haben und kann zu einer Beeinträchtigung ihrer Sicherheit sowie generell für humanitäre Maßnahmen führen.

Die US-amerikanische Federal Trade Commission enthält sich bei dieser Entschließung der Stimme, da sie Angelegenheiten außerhalb ihrer Zuständigkeit betrifft.

Entschließung über die internationale Zusammenarbeit der Aufsichtsbehörden

– nichtamtliche Übersetzung –

Die 38. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre:

In der Erkenntnis, dass durch die internationale Zusammenarbeit der Aufsichtsbehörden eine höhere Effizienz im regulatorischen Umfeld erreicht werden kann, die sowohl den Grad der Einhaltung durch datenverarbeitende Organisationen als auch die Wettbewerbsfähigkeit dieser Organisationen verbessern kann, was wiederum positive Folgen für Einzelpersonen hervorbringt;

In der Erkenntnis, dass die internationalen Aufsichtsbehörden große Fortschritte beim Knüpfen neuer Kontakte, dem Austausch von Wissen und der Entwicklung

neuer Instrumente zur Stärkung der gegenseitigen Zusammenarbeit in den letzten zehn Jahren erzielt haben, aber dass noch mehr getan werden kann. Aktuelle Fälle mit grenzübergreifendem Bezug leiden manchmal immer noch an rechtlichen Beschränkungen, die wirksame Fortschritte bei Ermittlungen behindern, und daher benötigen die Behörden alle Möglichkeiten zur Wahrung der Rechte des Einzelnen in Bezug auf den Schutz der Daten und der Privatsphäre. Die Mitglieder der Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre benötigen eine Vielzahl zur Verfügung stehender Möglichkeiten, die ihnen eine Zusammenarbeit erlauben, und sie sind dazu verpflichtet, dementsprechend im Einklang mit den für ihre Tätigkeiten geltenden Rechtsvorschriften zu handeln.

Unter Hinweis auf die Entschließungen der 29., 31., 33., 34., 35. und 36. Konferenz im Zusammenhang mit Maßnahmen zur Verbesserung der grenzüberschreitenden Zusammenarbeit der Aufsichtsbehörden;

Erinnert ferner daran, dass sich die 33. Konferenz entschloss, dafür zu sorgen, dass jedes Jahr mindestens einmal die Möglichkeit eines Treffens für diejenigen besteht, die sich für Fragen der internationalen Durchsetzung und Koordinierung des Schutzes der Privatsphäre interessieren; außerdem unter Betonung des Erfolgs der nachfolgenden Treffen in Kanada, den Vereinigten Staaten von Amerika und dem Vereinigten Königreich in den vergangenen fünf Jahren zum Erfahrungsaustausch und zur Entwicklung von Untersuchungs- und Durchsetzungsmethoden, die auf Instrumenten basieren, die gemeinsam von Konferenzmitgliedern erarbeitet worden sind, wie zum Beispiel einem Handbuch über die internationale Zusammenarbeit der Aufsichtsbehörden;

Unter Hinweis auf die konkreten Beispiele für den Erfolg der globalen Vereinbarung zur grenzübergreifenden Zusammenarbeit der Aufsichtsbehörden, soweit sie zwischen den Teilnehmern an der Veranstaltung der internationalen Aufsichtsbehörden im Vereinigten Königreich im Jahr 2016 mitgeteilt wurden;

Unter Hinweis darauf, dass, obwohl die Konferenz in ihren vergangenen Entschließungen einen weltweit geltenden Standard für den Datenschutz gefordert hat, einige Konferenzmitglieder aufgrund von Beschränkungen durch ihre nationalen oder regionalen Rechtsvorschriften noch nicht in der Lage sind, fallbezogene Daten miteinander zu teilen, und dass angesichts dieser Situation die Konferenz die Mitglieder in ihrer Arbeit auf nationaler Ebene mit gemeinsam vereinbarten Materialien über die internationale Zusammenarbeit der Aufsichtsbehörden unterstützen sollte. Die Mitglieder sollten diese Materialien ihren Gegebenheiten entsprechend an nationale, regionale und lokale Bedürfnisse anpassen können. Die Konferenz sollte ebenfalls deren Forderungen nach der Änderung der nationalen Rechtsvorschriften unterstützen;

Erinnert daran, dass die 36. Konferenz die globale Vereinbarung zur grenzübergreifenden Zusammenarbeit der Aufsichtsbehörden als Möglichkeit für jeden Teilnehmer an der Vereinbarung akzeptierte, um einen gemeinsamen Ansatz zur Erleichterung der Zusammenarbeit der Aufsichtsbehörden mit anderen Teilnehmern zu finden. Den Teilnehmern wurde dabei auch ein optionaler Anhang dieser Vereinbarung zur Verfügung gestellt, der diesen Teilnehmern die Erklärung ermöglicht, ob sie beabsichtigen, personenbezogene Daten in Zusammenhang mit grenzüberschreitenden Untersuchungen zu teilen, soweit nationale oder regionale Rechtsvorschriften dies zulassen;

In der Erkenntnis, dass der Exekutivausschuss der 37. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre die Mechanismen zur Operationalisierung der globalen Vereinbarung zur grenzübergreifenden Zusammenarbeit der Aufsichtsbehörden lieferte, die gemäß der Paragraphen 12–15 dieser Regelung notwendig sind, wobei diese auch eine Aktualisierung der Geschäftsordnung der Konferenz zur Anpassung an dieses neue Instrument enthielten;

Unter Hinweis darauf, dass die Empfehlung der OECD zur grenzübergreifenden Zusammenarbeit bei der Anwendung von Rechtsvorschriften zum Schutz der Privatsphäre ihren Mitgliedstaaten rät, Schritte zur Verbesserung der Kooperationsfähigkeiten ihrer Datenschutzbehörden zu unternehmen, auch indem den Behörden Verfahren zum Austausch von Informationen mit ausländischen Behörden zur Verfügung gestellt werden, und indem den Behörden die Unterstützung ausländischer Behörden ermöglicht wird, insbesondere im Hinblick auf die Erlangung von Informationen von Personen, von Unterlagen oder Datensätzen; oder in Bezug auf die Ortung oder Identifizierung von beteiligten Organisationen oder Personen oder von Dingen;

Unter Hinweis darauf, dass die 36. Konferenz den Exekutivausschuss beauftragt hatte, Gespräche mit GPEN und anderen Netzwerken aufzunehmen im Hinblick auf die Sondierung praktischer Möglichkeiten und Chancen für eine bessere Koordinierung ihrer Bemühungen zur Verbesserung der Zusammenarbeit der Aufsichtsbehörden, und dass der Ausschuss auf der 37. Konferenz über die Fortschritte Bericht erstattet hat;

In Anbetracht dessen, dass das Global Privacy Enforcement Network (GPEN) am Rande der 37. Konferenz den Startschuss für das neue GPEN Alarm-System gegeben hat, das den teilnehmenden Behörden die Benachrichtigung anderer teilnehmender Behörden über ihre datenschutzrechtlichen Untersuchungen und Durchsetzungsmaßnahmen ermöglicht, insbesondere über diejenigen, die grenzüberschreitende Aspekte aufweisen, für die Zwecke der möglichen Koordinierung und Zusammenarbeit; ferner unter Hinweis darauf, dass die Konferenz, GPEN und anderen Netzwerke sich gegenseitig über solche Projekte zur Förderung der

grenzüberschreitenden Zusammenarbeit auf dem Laufenden halten und die Diskussion über künftige Projekte begonnen haben;

Unter Hinweis darauf, dass es von mehreren anderen Netzwerken, die sich dem Schutz der Daten und der Privatsphäre widmen, Bemühungen zur Förderung der Teilnahme an internationalen Koordinierungsmaßnahmen von Aufsichtsbehörden aus Ländern mit weniger gut entwickelten Regelungen zum Schutz der Daten und der Privatsphäre auf der ganzen Welt gab.

Die 38. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre ist entschlossen, Bemühungen um eine wirksamere Zusammenarbeit bei grenzüberschreitenden Untersuchungen und von Aufsichtsbehörden in geeigneten Fällen weiterhin zu fördern und:

1) Eine neue Arbeitsgruppe, bestehend aus Experten und interessierten Mitgliedern der Internationalen Konferenz, und idealerweise aus Vertretern von Konferenzmitgliedern aus verschiedenen Weltregionen, mit der Ausarbeitung eines Vorschlags für entscheidende Grundsätze in Rechtsvorschriften zu beauftragen, um zwischen ihren Mitgliedern eine Zusammenarbeit der Aufsichtsbehörden zu erleichtern. Die Grundsätze könnten von einzelnen Mitgliedern an ihre nationalen, regionalen und lokalen Bedürfnisse angepasst werden. Die Grundsätze würden von einem erläuternden Bericht begleitet, der von einzelnen Mitgliedern ihren nationalen Regierungen, und gegebenenfalls Beobachtern, vorgelegt werden kann. Darüber hinaus wird die Arbeitsgruppe aufgefordert, Maßnahmen vorzuschlagen, die ihrer Ansicht nach die wirksame grenzübergreifende Zusammenarbeit auf kurze oder lange Sicht verbessern können. Die Arbeitsgruppe wird angeregt zur Zusammenarbeit mit anderen Netzwerken von Datenschutzbehörden, die im Bereich der grenzüberschreitenden Zusammenarbeit der Aufsichtsbehörden tätig sind, und sie soll gegebenenfalls Netzwerke von Aufsichtsbehörden aus anderen Sektoren zu Rate ziehen, und sie wird ferner angewiesen, der 39. Konferenz über das Ergebnis ihrer Arbeit Bericht zu erstatten.

2) Den Exekutivausschuss der Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre zu beauftragen, leitende Teilnehmerbehörden aus den einzelnen Weltregionen als Ansprechpartner für die Förderung der Teilnahme der Mitglieder der Internationalen Konferenz an der globalen Vereinbarung zur grenzübergreifenden Zusammenarbeit der Aufsichtsbehörden zu benennen;

3) Den Exekutivausschuss der Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre zu beauftragen, weitere Gespräche mit GPEN und anderen einschlägigen Netzwerken zu führen, um praktische

Projekte zur besseren Koordinierung der Bemühungen um eine weltweite Zusammenarbeit der Aufsichtsbehörden zu schaffen, insbesondere im Anschluss an die Schlussfolgerungen der jährlichen Veranstaltung zur internationalen Zusammenarbeit der Aufsichtsbehörden aus dem Jahr 2016, die die Überprüfung der Realisierbarkeit der Zusammenarbeit von Netzwerken zur Einrichtung einer Datenbank empfiehlt, die die rechtlichen Befugnisse der einzelnen Behörden zur Zusammenarbeit, die Vorschriften zur Nachweiserhebung, Definitionen von personenbezogenen Daten und vertraulichen Daten umfasst, und die den Konferenzmitgliedern die Identifizierung von Partnerbehörden in einem Fall erleichtern kann.

V. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 59. Sitzung am 24./25. April 2016 in Oslo, Norwegen

Aktualisierung zu Datenschutz und Datensicherheit in der Internettelefonie (Voice over IP VoIP) und verwandten Kommunikationstechnologien

– Übersetzung –

Einleitung

Im September 2006 veröffentlichte die Arbeitsgruppe ein Arbeitspapier zu Voice over IP (VoIP)-Anwendungen[1] in dem Bestreben, mögliche Datenschutz- und Datensicherheitsrisiken zu antizipieren. Dieses Papier schilderte die Situation, wie sie von der Arbeitsgruppe zu dieser Zeit gesehen wurde: Es beschrieb die sich entwickelten Dienste sowie mögliche zukünftige Datenschutz- und Datensicherheitsrisiken und enthielt eine Reihe von datenschutz- und datensicherheitsbezogenen Empfehlungen für Geräteherstelle, Softwareentwickler und Anbieter von VoIP-Diensten.

In den nachfolgenden zehn Jahren hat VoIP weitverbreitete Anwendung in Organisationen und bei Endnutzern gefunden. Darüber hinaus ist die Sprachtelefonie mit einer Reihe anderer Kommunikationstechnologien zusammengeführt worden, wie Instant Messaging und Text- und Videoübertragung. In einigen Regionen haben bereits Diskussionen über die Ausmusterung des „Plain Old Telephone System" (POTS) begonnen, das jetzt von einigen als „veraltete Infrastruktur" bezeichnet wird.

Die Empfehlungen in diesem Arbeitspapier gelten für alle Arten von Multimedia-Diensten, einschließlich Instant Messaging, Real-Time Text und Videodienste.[2] Darüber hinaus unterscheidet dieses Arbeitspapier nicht zwischen einem VoIP-Dienst, der von einem Telekommunikationsdiensteanbieter angeboten wird und dem Angebot eines „Over-the-Top"-Anbieters. Auch wenn sich die von den verschiedenen Unternehmen verwendete Technologie unterscheidet, bleiben die Datenschutz- und Datensicherheitsrisiken gleich und deswegen richten sich die Empfehlungen an all diese Unternehmen. Zusätzlich zu Standardlösungen exis-

[1] Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation: „Arbeitspapier zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP)", verabschiedet auf der 40. Sitzung am 5. – 6. September 2006 in Berlin (Deutschland); http://www.datenschutz-berlin.de/attachments/101/WP_VoIP_de.pdf

[2] Wir nutzen die Begriffe „Sprache und Video" und „Multimedia" synonym, da sich der Inhalt dieser Empfehlungen auf das allgemeinere Konzept von Multimedia-Kommunikation bezieht. Aus historischen Gründen und um die Lesbarkeit zu verbessern wird häufiger der Begriff Sprachtelefonie benutzt.

tieren viele proprietäre Produkte und Dienste, die einen unterschiedlichen Grad an Sicherheit, Datenschutz und Schutz der Privatsphäre bieten. Unglücklicherweise bleiben nicht-technische Nutzer über den gebotenen Schutz oft uninformiert, oder ihnen werden keine datenschutzfreundlichen Standardeinstellungen geboten.

Mit diesem zusätzlichen Arbeitspapier aktualisiert die Arbeitsgruppe die Empfehlungen, die in der ursprünglichen Veröffentlichung enthalten sind, auf Basis einer Neuevaluierung des heutigen Entwicklungsstandes (2016). Die folgenden Überlegungen motivieren die Neuevaluierung dieser Thematik:

- Die Enthüllungen von Edward Snowden deuten darauf hin, dass Strafverfolgungsbehörden und Geheimdienste rund um den Erdball in nie dagewesener Weise Zugriff auf VoIP-Verbindungen und auch auf die damit zusammenhängenden Verkehrsdaten haben – mit oder ohne Kooperation von Unternehmen, die diese Dienste im Internet anbieten (einschließlich Anbietern von VoIP-Diensten). Diese globale Überwachung stellt das Vertrauen sowohl in Entwickler als auch in Dienstanbieter in Frage. Informationslecks bei Verkehrsdaten, wie IP-Adressen, DNS-Anfragen und Adressköpfen der Anwendungsschicht (Signalling Header), stellen in gleicher Weise eine Herausforderung für die Vertraulichkeit der Kommunikation dar.[3] Zwar werden durch Verkehrsdaten keine Kommunikationsinhalte bekannt, sie liefern aber oft genügend Informationen über die kommunizierenden Partner, um deren Privatsphäre zu gefährden.

- Die Standardisierung im Bereich von VoIP hat Fortschritte gemacht und der Markt ist heutzutage weiter entwickelt als 2006, als das ursprüngliche Papier veröffentlicht wurde. Die Standardisierung des Session Initiation Protocol (SIP) und der verschiedenen Erweiterungen ist abgeschlossen und viele Produkte sind nunmehr auf dem Markt erhältlich. Zusätzlich ist mit Web-Real-Time-Communication (WebRTC)[4] ein neuer Standardisierungsversuch gestartet worden, der darauf zielt, eine bessere Harmonisierung mit Web-Technologien (und besonders mit Browsern) zu ermöglichen. Erste Anwendungen sind verfügbar. Das Ziel von WebRTC ist, die einfachere Integration von Echtzeitkommunikation in den Browser zu ermöglichen. Dies führt zu neuen Herausforderungen für Datenschutz und Datensicherheit[5].

- Der Einsatz von breitbandiger Mobilfunktechnologie und WiFi-Netzwerken hat substantiell zugenommen. Nutzer können diese Netzwerke für verlässli-

[3] R. Barnes, et al., „Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement" (RFC 7624), August 2015, abrufbar unter http://tools.ietf.org/html/rfc7624

[4] W3C, WebRTC 1.0: Real-Time Communication Between Browsers, abrufbar unter http://www.w3.org/TR/webrtc/

[5] E. Rescorla, „WebRTC Security Architecture", IETF draft (work in progress), März 2015, abrufbar unter https://tools.ietf.org/html/draft-ietf-rtcweb-security-arch-11

che VoIP- und Video-Verbindungen von hoher Qualität verwenden. Außerdem ist einfach zu bedienende VoIP-Software auf Endgeräten vorinstalliert, oder sie kann über App-Stores heruntergeladen werden. Wurde VoIP In den frühen 2000er Jahren überwiegend von Unternehmen und technisch versierten Nutzern verwendet, ist dies heute unter normalen Endnutzern weit verbreitet.

- Datenschutz- und Datensicherheitspraktiken der verschiedenen Angebote unterscheiden sich erheblich. Unglücklicherweise werden Nutzer über diese Praktiken nicht ausreichend informiert.

- POTS wurden traditionell von einem einzigen – in der Regel staatlichen – Anbieter installiert und verwaltet. Im Gegensatz dazu entwickelt sich die jetzige VoIP-Umgebung zu einer Zusammensetzung vieler Teile (z. B. Netzwerkdienste, Betriebssysteme, Anwendungssoftware). Diese „Teile" werden häufig von unterschiedlichen Einrichtungen entwickelt und verwaltet (z. B. dem Netzanbieter, dem Entwickler der Hard- oder Software und dem Hersteller des Geräts), die unabhängig voneinander und in den meisten Fällen ohne jegliche Koordination handeln. Während diese Vermehrung der Rollenden den Nutzern eine größere Auswahl ermöglichen könnte, führen die Anreize für die Beteiligten und ihre Ziele nicht notwendigerweise zu einer Verbesserung des Schutzes der Privatsphäre, da jeder Teilnehmer auf seinen Teil in der Kette fokussiert ist.

Technischer Hintergrund

Von der Konzeption her sind VoIP-Lösungen ziemlich einfach: Ein Nutzer gibt die Telefonnummer oder ein anderes Identifizierungsmerkmal (von denen viele wie eine E-Mail-Adresse aussehen) ein, um andere Nutzer „anzurufen". Mithilfe einer unterstützenden Infrastruktur, manchmal Proxies genannt, initiiert der VoIP-Klient dann die Kommunikationssignalisierung, um das Gerät des Angerufenen aufzufinden. Die Nachrichten, die im Rahmen dieser Prozedur ausgetauscht werden, werden als Signalisierungsnachrichten bezeichnet.

Für VoIP-Lösungen, die das Zusammenwirken mit anderen Anbietern nicht unterstützen, müssen alle Nutzer ihre Geräte bei demselben VoIP-Anbieter registriert haben. In offeneren Systemen kann dieser Erkennungsschritt kompliziert sein, weil Nutzer bei verschiedenen VoIP registriert sein können und die Erkennungsprozedur auf weitere Anbieter ausgedehnt werden kann. Es ist darauf hinzuweisen, dass das Zusammenwirken mit anderen VoIP-Systemen oder sogar mit dem öffentlichen Telekommunikationsnetz zu einem Verlust an Funktionalität und schwächeren Privatsphäre- und Sicherheitseigenschaften führen kann.

Wenn das Gerät des anderen Kommunikationspartners gefunden worden ist, können Sprachpakete zwischen den beiden Parteien ausgetauscht werden. Während

Signalisierungsnachrichten häufig indirekt über die unterstützende Infrastruktur zwischen den beiden Parteien geroutet werden, wird Multimedia-Verkehr (wie Sprach- und Videotelefonie) idealerweise direkt übertragen. Diese direkte Kommunikation führt zu geringerer Latenz. Sprachpakete können als Inhalt in dem „Secure Real-Time Transport Protocol" (SRTP)[6] eingekapselt sein. Es existieren verschiedene Protokolle, um dem überall vorhandenen Überwachungsrisiko zu begegnen.[7]

In praktischen Szenarien bieten Signalisierungsnachrichten mehr Funktionalität als das pure Auffinden von Kommunikationsgeräten, einschließlich der Aushandlung von Protokollparametern und Funktionen. Für anspruchsvollere Nutzungsszenarien, wie Konferenzschaltungen oder Rufweiterleitungen, kann die Prozedur zur Verbindungsherstellung komplexer sein. Für das Angebot von Kanalsicherheit mit SRTP ist außerdem die Einrichtung von kryptografischen Schlüsseln und Algorithmen erforderlich. Daher sind verschiedene unterschiedliche Schlüsselmanagement-Protokolle für die Einrichtung der zur Sicherung des medialen Verkehrs benötigten Schlüssel entwickelt worden, die alle geringfügig verschiedene Eigenschaften haben.[8]

Empfehlungen[9]

Im Lichte des oben Gesagten gibt die Arbeitsgruppe den verschiedenen Parteien folgende Empfehlungen:

Gesetzgeber und Regulierungsbehörden

Gesetzgeber und Regulierungsbehörden auf nationaler, regionaler und sogar globaler Ebene werden daran erinnert, dass im gesetzlichen Schutz der Vertraulichkeit der Kommunikation auf den verschiedenen Regulierungsebenen im Hinblick auf VoIP-Dienste Lücken existieren. Sie werden aufgerufen, die gesetzliche Situation gründlich zu untersuchen und die notwendigen Änderungen vorzunehmen, um sicherzustellen, dass die Bestimmungen zum Fernmeldegeheimnis, die in vielen nationalen Verfassungen und regionalen und globalen Regulierungsinstrumenten vorhanden sind, auch VoIP und andere Multimedia-Kommunikationsdienste vollständig abdecken.

---

[6] M. Baugher, et al., „The Secure Real-Time Transport Protocol (SRTP)", März 2004, RFC 3711, abrufbar unter https://tools.ietf.org/html/rfc3711

[7] IAB Statement on Internet Confidentiality, November 2014, abrufbar unter https://www.iab.org/2014/11/14iab-statement-on-internet-confidentiality/

[8] Für eine Analyse von Schlüsselaustausch-Technologien und ihren Eigenschaften siehe RFC 5479 (https://tools.ietf.org/html/rfc5479) und RFC 7201 (https://tools.ietf.org/html/rfc7201)

[9] Die Empfehlungen zu VoIP sind zusammen mit denen aus dem ersten Arbeitspapier der Gruppe von 2006 zu lesen; vgl. http://www.datenschutz-berlin.de/attachments/102/WP_VoIP_de.pdf

VoIP-Anbieter, Software-Entwickler und Hardware-Hersteller

Transparenz

VoIP-Diensteanbieter sollten ihre Kunden über die Datenschutz- und Datensicherheits-Charakteristiken der von ihnen angebotenen VoIP-Dienste informieren.

Datenschutzfolgeabschätzung und Evaluierung durch Dritte

Hersteller von Hard- und Software sollten Datenschutzfolgeabschätzungen durchführen. Die Arbeitsgruppe befürwortet auch die Analyse und Überprüfung durch unabhängige, vertrauenswürdige Dritte. Ein Beispiel einer solchen Untersuchung ist die „Secure Messaging Scorecard" der Electronic Frontier Foundation (EFF).[10] Automatische Werkzeuge werden zum Beispiel von der XMPP Foundation[11] und der GSM Map[12] angeboten.

Design-Überlegungen

Software-Entwickler und Hardware-Hersteller sollten angemessene technische Maßnahmen ergreifen, um den Signalisierungs-Verkehr wie auch den Sprach- und Videotelefonie-Verkehr gegen die weit verbreitete unautorisierte Überwachung zu schützen. Dazu ist es als grundlegende Design-Überlegung unerlässlich, dass Software-Entwickler Implementierungen auf Basis von Ende-zu-Ende-Verschlüsselung sowohl für die Signalisierung als auch für den Inhalt anstreben.

Der VoIP-Signalisierungsverkehr muss authentisiert und Integrität und Vertraulichkeit müssen zwischen den teilnehmenden VoIP-Signalisierungsknoten geschützt werden. Die Bereitstellung von Ende-zu-Ende-Integrität für den gesamten VoIP-Signalisierungsverkehr ist bedauerlicherweise in den meisten VoIP-Architekturen nicht möglich, weil die Signalisierungs-Nutzdaten bei der Übertragung verändert werden.[13] Die Übertragung von Signalisierungs-Nachrichten über Verbindungen, die nicht kryptografisch geschützt sind, sollte vermieden werden. Es ist darauf hinzuweisen, dass es angesichts des Ausmaßes allgegenwärtiger

[10] Electronic Frontier Foundation (EFF), „Secure massaging Scorecard", Oktober 2015, abrufbar unter https://www.eff.org/secure-messaging-scorecard

[11] XMPP(Extensible Messaging and Presence Protocol) Foundation, „XMPP Security Tests", Oktober 2015, abrufbar unter http://xmpp.net

[12] GSM – *Global System for Mobile Communications* (vorher „Groupe Spécial Mobile"). Vgl. Karsten Nohl, „GSM Map", Oktober 2015, abrufbar unter https://gsmmap.org

[13] Da die Modifizierung der Nutzdaten von Signalisierungsnachrichten Signaturalgorithmen bricht, wie auf S. 16 des RFC 7340 beschrieben (https://tools.ietf.org/html/rfc7340) und die meisten VoIP-Architekturen Signalisierungs-Nutzdaten bei der Übertragung modifizieren, muss die Anzahl der teilnehmenden Knoten so klein wie möglich gehalten werden, um die Integrität des gesamten VoIP-Signalisierungsverkehrs sicherzustellen. RFC 7044 bietet eine Lösung zur stufenweisen Anwendung von Nachrichtenschutz („message protection"), während die Nachrichten durch das SIP-Kommunikations-Netzwerk geroutet werden. Dies bietet der kommunizierenden Partei Informationen über den Verlauf (https://tools.ietf.org/html/rfc7044).

Überwachung im heutigen Internet keine angemessene, dem Stand der Technik entsprechende Sicherheitstechnik ist, sich allein auf die physische Sicherheit zu verlassen.[14]

Verkehrsdaten über die Kommunikation, wie die Identifikatoren der kommunizierenden Parteien, Kommunikations-Präferenzen (wie Codecs und Sprache), Länge der (verschlüsselten) Datenpakete und Online-Status verraten oft eine überraschende Menge an Informationen. Die Arbeitsgruppe empfiehlt daher, den Umfang der Daten zu begrenzen, der Intermediären, wie z. B. Signalisierungs-Gateways, zugänglich gemacht wird, und die Verwendung persistenter Identifikatoren soweit wie möglich zu vermeiden.

Die Arbeitsgruppe ermutigt VoIP-Anbieter nachdrücklich, Schlüsselmanagement-Mechanismen zu verwenden, die es Intermediären nicht erlauben, an Schlüsselmaterial zu gelangen (weil es im Klartext eingebettet in die Signalisierungs-Nachrichten übertragen wird), und ein Schlüsselmanagement-Protokoll zu verwenden, das „Perfect Forward Secrecy" (PFS)[15] benutzt. PFS ist ein Sicherheitsmerkmal, das die Entschlüsselung zurückliegender Konversationen durch Kompromittierung der geheime Schlüssel innerhalb längerer Zeiträume durch einen Angreifer verhindert. Trotz der Beschränkungen einiger VoIP-Architekturen sollte die Priorität auf die Implementierung von Ende-zu-Ende-Sicherheit für Sprach- und Videokommunikation gelegt werden.

Es sollten Maßnahmen entwickelt werden, mit denen Nutzer durch Verifizierung der Schlüssel nachprüfen können, ob ein „Man-in-the-middle"-Angriff stattgefunden hat, soweit Zertifikate zum Aufbau der Ende-zu-Ende-Kommunikation erforderlich sind. Zertifikat[16] könnten durch vertrauenswürdige Dritte ausgegeben und könnten – als Option – mit Pseudonymen (Telefonnummer, Nutzername, oder Namen von Organisationen) verbunden werden, die den kommunizierenden Parteien angezeigt werden.

VoIP-Diensteanbieter müssen standardmäßig den Umfang der personenbezogenen Daten, die sie speichern und verarbeiten, auf das für die Erbringung und Abrechnung (falls zutreffend) des Dienstes Notwendige beschränken, soweit eine zusätzliche Speicherung und Verarbeitung von Daten nicht ausdrücklich durch Gesetz vorgeschrieben ist. Der Schutz gespeicherter Daten gegen unautorisierten Zugriff muss sichergestellt werden.

---

[14] Während die für „klassische" Telekommunikationsdienste genutzte Leitungs-Infrastruktur als „sicher per Definition" angesehen wurde, kann diese Annahme nicht mehr weiter gelten: Heutzutage werden Leitungen in großem Umfang von Geheimdiensten abgehört.

[15] Die PFS-Eigenschaften sind genauer erklärt in https://en.wikipedia.org/wiki/Forward_secrecy. Vgl. auch A. Menezes, P van Oorschot, und S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, USA 1996 (S. 496).

[16] J.Peterson, et al., „Secure Telephone Identity Credentials: Certificates", IETF draft (work in progress), März 2016, abrufbar unter https://tools.ietf.org/html/draft-ietf-stir-certificates-03

VoIP-Diensteanbieter müssen grundlegende datenschutzrelevante Leistungsmerkmale, wie Rufnummernunterdrückung, wenigstens in derselben Art und Weise anbieten, wie dies in Fest- und Mobilfunknetzen üblich ist. Da die Unterdrückung der Rufnummer und das „Caller ID Spoofing" bestimmte Arten von Angriffen ermöglicht, sollten kürzlich entwickelte Schutzmechanismen berücksichtigt werden.[17] Die Unterdrückung der Rufnummerninformation macht Zugriffskontrolllisten, manchmal auch Freundeslisten genannt, weniger effektiv. Aufgrund der direkten Verbindung zwischen den Kommunikationspartnern werden ihnen die jeweiligen IP-Adressen bekannt. Um dies zu verhindern, sollte die optionale Nutzung von Proxies oder Anonymisierungsdiensten (z. B. Tor[18], TURN[19]) nicht verboten werden.

Vorhandene, offene Standards, die Gegenstand von umfassender Überprüfung und Verifikation durch eine große Zahl unabhängiger Experten gewesen sind, sollten wiederverwendet werden. Für den Schutz von Sprachkommunikation sind mehrere standardisierte Lösungen verfügbar.[20,21] Es ist darauf hinzuweisen, dass der Standardisierungsprozess in verschiedenen Organisationen die Veröffentlichung technischer Spezifikationen ohne eine signifikante Überprüfung durch Experten erlaubt oder, im schlimmsten Fall, sogar ohne jegliche Überprüfung. Daher sollte eine Entscheidung darüber, welche technische Spezifikation genutzt werden soll, den Grad der Überprüfung in Betracht ziehen. Standardisierungsorganisationen werden ermutigt, für mehr Transparenz über den Prozess zu sorgen, durch den eine Spezifikation entwickelt worden ist.

Nutzerbeteiligung

VoIP-Anbieter sollten ihren Nutzern ermöglichen, ihren eigenen Identitäts-Anbieter zu wählen, wo solch eine Trennung zwischen Identitäts-Anbieter und VoIP-Diensteanbieter technisch möglich ist.

VoIP-Anbieter sollten (wo dies angemessen ist) Datenportabilität anbieten, um ihren Kunden einen bequemen Zugriff auf relevante Daten, wie Freundeslisten und Konfigurationsdaten zu ermöglichen.

---

[17] IETF, „Secure Telephone Identity Revisited (STIR) Working Group", Oktober 2015, abrufbar unter https://datatracker.ietf.org/wg/stir/charter/

[18] Weitere Informationen über die Onion-Routing-Technologie Tor sind verfügbar unter https://en.wikipedia.org/wiki/Tor_(anonymity_network)

[19] R. Mahy, et al., „Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, April 2010, abrufbar unter https://tools.ietf.org/html/rfc5766

[20] M. Westerlund und C. Perkins, „Options for Securing RTP Sessions", RFC 7201, April 2014, abrufbar unter https://tools.ietf.org/html/rfc7201

[21] D. Wing, et al., „Requirements and Analysis of Media Security Management Protocols", RFC 5479, April 2009, abrufbar unter https://tools.ietf.org/html/rfc5479

Operationale Überlegungen

Alle Akteure in der Lieferkette müssen schnell auf Datensicherheits- und Datenschutz- Schwachstellen in den Protokollen und der genutzten Hard- oder Software reagieren. Für Schwachstellen in verteilter Software, wie Smartphone-Apps oder herunterladbarer Software, erfordert dies einen Software-Update-Mechanismus.

VoIP-Dienstanbieter müssen sicherstellen, dass Datenschutz- und Datensicherheitsmerkmale ihrer Produkte standardmäßig aktiviert sind. Datenschutz- und Datensicherheitsmechanismen sollten dem Kunden ohne prohibitive Kosten angeboten werden.

VoIP-Dienstanbieter sollten einen föderierten Zugang (federated access) zu ihren VoIP-Diensten anbieten. Dies ermöglicht es Nutzern, sich mit Nutzern anderer VoIP-Anbietern zu verbinden, ohne verschiedene VoIP-Klienten herunterzuladen und installieren zu müssen. Als Minimum müssen Nutzer über Veränderungen von Sicherheits- und Datenschutzeigenschaften ihrer Kommunikation beim „Interworking“ mit anderen VoIP-Systemen (oder sogar dem öffentlichen Telefonnetz) informiert werden und über jeden Verlust von Funktionalität, Sicherheit oder Schutz der Privatsphäre, der aus solchen Veränderungen entstehen kann.

Zweckbindung

Anbieter, Software-Entwickler und Hardware-Hersteller, die Verkehrsdaten verarbeiten, müssen das Prinzip der Zweckbindung respektieren.

Nutzer

Nutzer von VoIP-Diensten sollten die möglichen Risiken für die Sicherheit und die Privatsphäre ihrer Kommunikation berücksichtigen. Sie sollten sich über Sicherheits- und Datenschutzeigenschaften der verschiedenen Dienste informieren, und die von ihnen genutzten Dienste und Dienstanbieter danach auswählen. Schließlich sollten Sie sicherstellen, dass existierende Sicherheits- und Datenschutzmechanismen eines Dienstes vor dessen Nutzung aktiviert werden.

Über die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“)

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (englisch: International Working Group on Data Protection in Telecommunications – IWGDPT, auch bekannt als „Berlin Group“) besteht aus Vertretern von

Datenschutzbehörden und Organisationen aus aller Welt, die sich mit dem Schutz der Privatsphäre beschäftigen. Die Arbeitsgruppe wurde 1983 im Rahmen der Internationalen Datenschutzkonferenz auf Initiative der Berliner Landesdatenschutzbehörde gegründet, die seither den Vorsitz führt. Seit ihrer Gründung hat die Arbeitsgruppe eine Vielzahl von Empfehlungen („Gemeinsame Standpunkte" und „Arbeitspapiere") zur Verbesserung des Schutzes der Privatsphäre in der Telekommunikation verabschiedet. Seit Anfang der neunziger Jahre beschäftigt sich die Gruppe insbesondere mit dem Schutz der Privatsphäre im Internet.

Weitere Informationen über die Arbeitsgruppe sowie die von der Gruppe verabschiedeten Dokumente sind auf der Webseite der Arbeitsgruppe abrufbar: http://www.berlin-privacy-group.org.

2. 60. Sitzung am 22./23. November 2016 in Berlin

Arbeitspapier zu Biometrie in der Online-Authentifizierung

– Übersetzung –

Einleitung

1. Das Management der Benutzeridentifizierung und des Zugangs zu Computersystemen ist von außerordentlicher Bedeutung, um die Sicherheit und die Funktionalität dieser Systeme sicherzustellen. Um Datenschutz und Datensicherheit zu gewährleisten, ist eine Zugangskontrolle erforderlich, damit sichergestellt wird, dass die richtigen Nutzer den richtigen Zugriff auf IT-Systeme und die dort gespeicherten persönlichen Daten erhalten. Eine kluge Abwägung der verschiedenen Facetten der Zugangskontrolle, d. h. der Identifikation, Authentifizierung und Autorisierung muss erfolgen, damit ein angemessenes Niveau von Sicherheit und Privatsphäre gewährleistet werden kann. Bei der Authentifizierung wird etwas, das mit der Person in Verbindung gebracht und durch sie kontrolliert wird (z. B. ein Passwort oder ein Token) eingesetzt, um eine behauptete Identität nachzuweisen. Im Vergleich hierzu wird bei der Identifizierung versucht, eine spezifische Person innerhalb einer Population (z. B. die Suche nach einer bestimmten Person in einer Menge) anhand ihrer Eigenschaften herauszugreifen.

2. Ein Beispiel für Authentifizierung: Wenn eine Person ein Gepäckstück bei einer Theatergarderobe abgibt, gibt sie sich als Eigentümer des Gepäckstückes zu erkennen. Keine weiteren Überprüfungen, etwa ob der anfängliche Eigentumsanspruch zutrifft, sind für das zuverlässige Funktionieren der Gar-

derobe erforderlich. Um sicherzustellen, dass die rechtmäßigen Eigentümer ihre Gepäckstücke zurückerhalten, muss das Personal vor der Rückgabe den Anspruch einer Person auf ihr Eigentum verifizieren. Häufig wird in diesem Zusammenhang **etwas, das die Person hat**, überprüft und zwar ein nummerierter Token, der ausgegeben worden ist, als das Gepäckstück abgegeben wurde. Als häufigste Methode der Authentifizierung für Online-Dienste wird etwas genutzt, **das der Person bekannt ist**, wie z. B. ein Passwort, um die Identität (hier die Angabe des Benutzernamens) zu authentifizieren. Eine weitere Authentifizierungsmethode, die häufig als Biometrie bezeichnet wird, besteht darin, **etwas** zu überprüfen, **das die Person ist** (ein physikalisches oder physiologisches Charakteristikum, z. B. ihr Gesicht) oder tut (ein verhaltensbezogenes Charakteristikum, z. B. ihre Unterschrift).

3. Verschiedene Authentifizierungsmethoden können kombiniert werden, um ein höheres Maß an Vertrauen in die Authentifizierung zu bieten oder um bekannten Bedrohungen und Schwachstellen zu begegnen. Ein typisches Beispiel ist die Verwendung einer PIN (etwas, das der Benutzer kennt) mit einer Kredit- oder Kundenkarte (etwas, das der Benutzer hat), um die Person als Besitzer des Bankkontos, das für den Kauf genutzt wird, zu authentifizieren. Die Auswahl der Authentifizierungsmethode (falls es eine gibt), die für eine bestimmte Aufgabe erforderlich ist, hat eine direkte Auswirkung auf das System, aber auch auf die Privatsphäre. Bei der Nutzung eines nummerierten Tokens in der Gepäckabgabe kann die Person anonym bleiben, aber es besteht ein Restrisiko, dass ein Betrüger die Tasche abholt. Durch die Nutzung eines Ticketdesigns, das extra für den Veranstaltungsort ausgegeben wird und den Vergleich des abgerissenen nummerierten Tickets mit der Nummer auf der Gepäckmarke der Tasche kann dieses Risiko als entsprechend gering angesehen werden, so dass die Benutzer kein Fingerabdrucksystem nutzen oder ein von einer Behörde ausgestelltes Ausweisdokument aushändigen müssen.

4. Passwörter haben als Methode, Nutzer als die Eigentümer eines Accounts zu authentifizieren, eine lange Geschichte in der IT. Sie sind für die Nutzer relativ bequem, da sie auf vielen verschiedenen Geräten genutzt werden können und einfach in die Online-Dienste zu integrieren sind.

5. Die weite Verbreitung von Online-Dienstleistungen bedeutet jedoch auch, dass eine Person Dutzende oder Hunderte von Nutzeraccounts haben kann. Folglich bringt die Geheimhaltung der Passwörter einige Herausforderungen mit sich, die dadurch entstehen, dass

   - Nutzer das gleiche Passwort auf verschiedenen Seiten benutzen;
   - Nutzer sich möglicherweise das Passwort mit Dritten teilen, um ihnen Zugang zu dem Account in ihrem Namen zu gestatten;

- Passwörter häufig vergessen werden, was Zeit und ressourcenintensive Wiederherstellungsmechanismen erfordert, die unsicher und anfällig für Angriffe sein können;
- ein Nutzer mit einer Vielzahl von Richtlinien konfrontiert werden kann, die Passwörter mit unterschiedlicher Länge und Zusammensetzung erfordern oder regelmäßige Änderungen erzwingen[1];
- Passwörter häufig unsicher gespeichert werden und
- Passwörter auf andere Art und Weise kompromittiert werden können (z. B. durch Phishing).

6. Als Folge ersetzen mehr und mehr Online-Dienste passwortbasierte Authentifizierung oder sie ergänzen sie mit einer sogenannten mehrstufigen Authentifizierung. Gängige Technologien, die eine mehrstufige Authentifizierung nutzen, bedienen sich:
   - eines Tokens oder einer App für Einmal-Passwörter,
   - vertrauenswürdiger Geräte (wie z. B. Chipcards)
   - oder der Biometrie.

7. Die Nutzung von Biometrie bei der Online-Authentifizierung bietet die Möglichkeit, etwas gegen einige der Mängel der jetzigen passwortbasierten Authentifizierung zu tun. Wie dieses Arbeitspapier jedoch im Weiteren beschreibt, muss der Datenschutz und die Datenschutzrisiken, die als Folge entstehen können, sorgfältig abgewogen werden.

8. Der Zweck dieses Arbeitspapieres besteht nicht darin aufzuzeigen, wann Biometrie als ein Faktor in der Online-Authentifizierung genutzt werden kann. Dies ist eine Entscheidung, die in einer Datenschutz-Folgenabschätzung dokumentiert werden sollte, die in der Planungsphase eines Projektes durchgeführt wird und während der gesamten Lebensdauer des IT-Systems aktualisiert werden muss. Dieses Arbeitspapier will auf die Risiken für die Privatsphäre hinweisen, die bei der Einführung von Biometrie und der Nutzung für die Authentifizierung entstehen, und wie diese Risiken angemessen gemanagt werden können.

[1] Empfehlungen der letzten Zeit legen nahe, dass regelmäßige Passwortänderungen zu einer Verminderung der Sicherheit der Passwörter führen können, da die Nutzer Passwörter wählen, an die sie sich leichter erinnern können, vgl. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach, https://www.cs.unc.edu/~reiter/ papers/2010/CCS.pdf, and http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/

Biometrie

9. Der Begriff *Biometrie* ist in der ISO/IEC 2382:2015[2] definiert als:

   „die Nutzung verschiedener Attribute, die einzigartige persönliche Merkmale wiedergeben, wie z. B. ein Fingerabdruck, ein Scan der Adernstruktur der Augennetzhaut oder Voiceprinting, um die Identität einer Person zu validieren."[3]

10. Seine Einzigartigkeit (innerhalb der Population der Nutzer) und die relative Einfachheit der Anwendung führen dazu, dass Biometrie zu einem attraktiven Kandidaten für die Authentifizierung wird. Bei der Anwendung von Biometrie bei der Authentifizierung handelt es sich nicht um einen neuen Trend, sondern eher um eine Weiterentwicklung der Technik wie der Analyse von Fingerabdrücken, die bereits lange in der Strafverfolgung für die Identifizierung eingesetzt wird. Heute werden biometrische Sensoren allerdings auch in Verbrauchergeräte eingebaut, am häufigsten kommen Fingerabdrucksensoren in Smartphones, Tablets und Laptops zum Einsatz. Zur Gesichts- und Stimmerkennung werden die eingebauten Kameras und Mikrophone genutzt.

11. Um einen Nutzer mit einem passwortbasierten System zu authentifizieren, wird durch eine einfache Rechenoperation verifiziert, ob der Nutzer das richtige Passwort verwendet hat. Dies führt zu einer unwiderlegbaren Ja- oder Nein-Antwort – ein Passwort ist entweder korrekt oder nicht. Biometrische Authentifizierung auf der anderen Seite folgt im Allgemeinen einer wahrscheinlichkeitstheoretischen Methode, bei der zwei Templates miteinander verglichen werden und eine prozentuale Übereinstimmung oder eine Vertrauenspunktzahl generiert wird. Ein Ergebnis oberhalb einer bestimmten Schwelle bestimmt, ob der Vergleich als eine positive Übereinstimmung gewertet werden kann oder nicht.

12. Um die Genauigkeit zu verbessern und die Möglichkeit für Spoofing zu verringern, kann das Authentifizierungssystem eine Mischung von mehr als einem biometrischen Charakteristikum benutzen oder biometrische und nichtbiometrische Daten der gleichen Person kombinieren. Abhängig vom Szenario kann es für eine erfolgreiche Authentifizierung notwendig sein, einen

[2] ISO/IEC 2382:2015 Information technology Vocabulary, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en

[3] Die Verordnung (EU) des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr definiert biometrische Daten als mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

positiven Vergleich über alle zur Verfügung gestellten Daten (biometrische und nicht-biometrische) zu erhalten, dies trifft aber nicht immer zu.

13. Nicht nur die Verbraucher interessieren sich mehr und mehr für die Verwendung von Biometrie als einer bequemen Authentifizierungsmethode, sondern auch Regierungen und Organisationen. So setzt sich z. B. die eIDAS-Verordnung der Europäischen Union (Verordnung über elektronische Identifizierung und Vertrauensdienste im internen Markt)[4] für die optionale Nutzung der Biometrie ein, um die Anwendung elektronischer Signaturen in ganz Europa zu unterstützen.

14. Fortgeschrittene Technologien zum Schutz der Privatsphäre schließen biometrische Verschlüsselung[5] und widerrufbare Biometrie[6] ein. Beide Techniken bieten verschiedene Vorteile gegenüber traditionellen biometrischen Systemen, im Besonderen die Widerrufbarkeit der gespeicherten biometrischen Daten. Außerdem wurde vor kurzem ein aus der Ferne einsetzbares biometrisches Authentifizierungsprotokoll vorgestellt[7], das gegenüber fortgeschrittenen Sicherheitsbedrohungen Widerstand zu leisten vermag. Dieses Protokoll bietet dann Sicherheit, solange höchstens entweder das Gerät des Nutzers oder der Server kompromittiert wurde (aber nicht, wenn dies bei beiden geschieht).

15. Aktivitäten auf dem Feld der Standardisierung innerhalb der FIDO Alliance[8] und ISO[9] sowie Verhaltensregeln wie die Privacy Trust Mark[10] des Biometrics Institute zielen auf Themen wie Sicherheit und Privatsphäre ab, indem sie robuste Authentifizierungsmechanismen fördern.

---

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014R0910&from=EN

[5] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar. Biometric Encryption. McGraw-Hill, 1999

[6] Widerrufbare Biometrie fügt dem gespeicherten Template eine wiederholbare Distorsion zu, vgl. z. B. Ruud M. Bolle, Jonathan H. Connell, und Nalini K. Ratha. Biometric perils and patches, volume 35, pages 2727-2738. Elsevier, 2002.

[7] Syta et al., Private Eyes: Secure Remote Biometric Authentication, 2015, http://dedis.cs.yale.edu/ dissent/ papers/ secrypt15-biometric.pdf

[8] https://fidoalliance.org/

[9] JTC 1/SC 37, http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home/jtc1_sc37_home.htm

[10] http://www.biometricsinstitute.org/pages/trust-mark.html

Datenschutzrisiken

16. Die Datenschutzrisiken in diesem Bereich wurden bereits durch verschiedene Datenschutzbeauftragte dokumentiert, einschließlich derer in der EU (2003[11] und 2012[12, 13]), Kanada[14] und den USA[15].

17. Schließlich ist darauf hinzuweisen, dass im Allgemeinen verschiedene biometrische Systeme sich sehr unterschiedlich auf Datenschutz und Schutz der Privatsphäre auswirken und daher einen unterschiedlichen Ansatz im Umgang mit diesen Risiken erforderlich machen. Gesichtserkennung kann z. B. bei Personen wirken, die nicht wissen, dass sie von diesem System betroffen sind, während Fingerabdrucksysteme normalerweise die aktive Beteiligung der Person erforderlich machen (obwohl dies nicht das gleiche sein kann wie die Zustimmung des Einzelnen). Ersteres kann daher größere Anstrengungen erforderlich machen, um die Nutzer über den Betrieb des Systems zu informieren.

18. Bestimmte biometrische Daten können von anderen ohne das Wissen des Einzelnen erworben werden – wir hinterlassen unsere Fingerabdrücke auf vielen Oberflächen, unsere Gesichter können erkannt werden, die entsprechenden Fotos können gespeichert und leicht weiterverarbeitet werden. Im Gegensatz zu Passwörtern sind biometrische Daten keine Geheimnisse und nicht einfach zu ändern oder zu widerrufen. Die Personen sind sich im Allgemeinen der Gefahren bewusst, die mit der Offenlegung eines Passwortes verbunden sind, aber man kann nur schwer verhindern, dass das Gesicht oder die Stimme aufgenommen wird.

19. Die Tatsache, dass biometrische Authentifizierung auf Wahrscheinlichkeit beruht (d. h. wie wahrscheinlich ist es, dass es bei der Abfrage mit dem angemeldeten Template ein Match gibt?) bedeutet, dass die Möglichkeit eines Irrtums besteht. Ein falsches negatives Match wird dazu führen, dass es unmöglich ist, die Person als korrekt zu authentifizieren, und ihr möglicherweise der Zugang zum System verweigert wird. Umgekehrt führt ein falsches positives Match dazu, dass eine Person fälschlicherweise authentifiziert wird oder ein Betrüger das System erfolgreich täuscht und dadurch unautorisierten Zugang zu dem System erhält. Die Fehlerraten müssen ein Gleichgewicht

[11] Working Document on Biometrics, August 2003, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

[12] Opinion 3/2012 on developments in biometric technologies , March 2012, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

[13] Opinion 02/2012 on facial recognition in online and mobile services, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

[14] Data at your fingertips, https://www.priv.gc.ca/information/pub/gd_bio_201102_e.pdf

[15] FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies, https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition

zwischen Benutzerfreundlichkeit und Sicherheit schaffen. Wenn die Schwelle zu hoch angesetzt ist, kann dies zu einer höheren Genauigkeit führen, aber mit einem damit verbundenen Anstieg an legitimen Nutzern, die nicht akzeptiert werden und umgekehrt. Dadurch kann die Versuchung entstehen, in einem unbedachten Kompromiss zwischen Benutzerfreundlichkeit und Performanz die Genauigkeitsrate zu senken, um so falsche Ablehnungsraten zu reduzieren, oder zu versäumen, das System unter realen Arbeitsbedingungen auf negative Auswirkungen auf die Sicherheit und Privatsphäre zu testen.

20. Bestimmte Geräte oder Komponenten, die in einem PC, Laptop oder Smartphone eingebaut sind, haben möglicherweise aufgrund des Drucks, die Produktionskosten zu senken, keine hohe Qualität. Diese Low-End-Sensoren können eine höhere Fehlerquote produzieren mit größeren Auswirkungen auf die Sicherheit und Privatsphäre für den Endverbraucher. Einige Systeme können durch gestohlene oder gefälschte biometrische Merkmale[16] getäuscht werden, falls mangelhafte Tests diese Fälschungen nicht zurückweisen.

21. Falls eine Person nicht in der Lage ist, eine verlässliches biometrisches Datum zu hinterlegen (z. B. durch abgenutzte oder beschädigte Fingerspitzen) oder weil sie aus einem anderen Grund nicht in der Lage oder nicht gewillt ist, das Aufnahmegerät zu nutzen (z. B. wenn das Gesicht durch einen Schleier, einen Schal oder Ähnliches bedeckt ist), kann dies zu einer regelmäßigen Zugangsverweigerung führen.

22. Biometrische Merkmale sind ebenso wie Passwörter nicht immun gegenüber unberechtigten Offenlegungen personenbezogener Daten. Das Hacken von mehr als 5,6 Millionen Fingerabdrücken aus dem Office of Personnel Management (OPM)[17] im Juni 2015 zeigt die potentielle Gefahr von zentral gespeicherten Anmeldeinformationen. Dieser Angriff war besonders ernst, da das OPM die Originalfingerabdrücke gespeichert hatte, statt Templates oder die digitale Darstellung der biometrischen Daten.

23. Biometrische Daten sind dauerhaft und können nicht leicht geändert oder erneut genutzt werden, wie dies der Fall bei einem unautorisierten Zugriff oder der Offenlegung von Passwörtern, Keycards oder Tokens ist. Während die Liste aller möglichen Passwörter, aus der eine Person wählen kann, unglaublich lang ist, gibt es eine niedrige und begrenzte Anzahl von Quellen, die für biometrische Daten eines Einzelnen genutzt werden können (d. h. zwei Retinas, 10 Fingerabdrücke und ein Gesicht). Daher gibt es ein reales Risiko, dass Nutzeraccounts bei verschiedenen Diensten verlinkt werden können (wenn bei ihnen derselbe Fingerabdruck hinterlegt worden ist). Dies

[16] Chaos Computer Club breaks Apple TouchID, https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

[17] https://www.opm.gov/cybersecurity/cybersecurity-incidents/ – Verwaltung des Öffentlichen Dienstes

spiegelt die gegenwärtigen Probleme der erneuten Verwendung von Passwörtern wider.

24. Die Verwendung von biometrischen Daten für die Authentifizierung kann die Möglichkeit der Nutzer, ein pseudonymes Konto zu nutzen, verringern. Dies reduziert die Verfügbarkeit von Dienstleistungen für Nutzer, die ihre wahre Identität dem Dienstleister nicht offenbaren möchten, oder Nutzer, die unterschiedliche Accounts für verschiedene Zusammenhänge (z. B. verschiedene Accounts für berufliche und private Zwecke) beibehalten möchten.

25. Die Verhinderung großflächiger Angriffe wie z. B. des unautorisierten Zugriffs auf Datenbanken, die biometrische Templates speichern, stand ebenso wie die Erleichterung der Anwendung biometrischer Systeme im Mittelpunkt der jüngsten Standardisierungsbemühungen. Datenschutzfreundlichere biometrische Systeme speichern biometrische Templates lokal auf den Geräten der Endnutzer wie z. B. einem Smartphone oder Tablet. Während diese Lösung es erforderlich macht, dass der Angreifer eine große Anzahl von Geräten eines nach dem anderen angreifen muss, muss auch bei der Implementierung dieser Lösung mit Bedacht vorgegangen werden, wie ein Sicherheitszwischenfall zeigte, bei dem es um Mobiltelefone ging, in denen biometrische Templates (Fingerabdruck) unverschlüsselt auf dem Filesystem[18] gespeichert wurden. Durch die lokale Speicherung von Templates auf den Geräten der Endnutzer werden sie darüber hinaus den Vorgehensweisen der Endnutzer selbst ausgesetzt[19], die ebenso wenig sicher sind.

26. Einige Hersteller biometrischer Systeme verlassen sich immer noch auf die Geheimhaltung der Algorithmen, die sie einsetzen, um Sicherheit und Vertrauen zu gewährleisten. Proprietäre Algorithmen und Technologien, die auf Geheimhaltung basieren, sind jedoch im Allgemeinen weniger vertrauenswürdig als diejenigen, die von Seiten Dritter überprüft wurden oder auf weithin akzeptierten Standards basieren[20].

Empfehlungen

27. Mit Blick auf das oben Gesagte gibt die Arbeitsgruppe den Interessenvertretern folgende Empfehlungen:

---

[18] Y. Zhang, et al. Fingerprints On Mobile Devices: Abusing and Leaking , Black Hat, August 2015, available at https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf

[19] Das „moralische Risiko“ anzunehmen, dass wir die volle Kontrolle über unsere Daten haben, kann zu unvorsichtigem Verhalten führen. Vgl. Misplaced Confidences: Privacy and the Control Paradox Laura Brandimarte, Alessandro Acquisti, George Loewenstein, In: Ninth Annual Workshop on the Economics of Information Security (WEIS), June 7–8 2010, Harvard University, Cambridge, MA

[20] Cf. https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data.

Regulierungsbehörden, Gesetzgeber und Aufsichtsbehörden

28. Regulierungsbehörden auf regionaler, nationaler und internationaler Ebene sollten die Entwicklung von datenschutzfreundlichen Authentifizierungstechnologien, die die Defizite der existierenden passwortbasierten Authentifizierungstechnologien beheben, unterstützen. Aus Sicht einer regulatorischen Vorgehensweise und standardisierten Sichtweise sollte darauf geachtet werden, dass bei der Behebung der in diesem Papier identifizierten Datenschutzrisiken diese mit den Risiken, die aus der Anwendung neuer Authentifizierungstechnologien entstehen, besonders, wenn es um sich um biometrische Technologien handelt, gegeneinander abgewogen werden.

29. Proaktive Vorgehensweisen des Datenschutzes wie z. B. die Durchführung von Datenschutz-Folgeabschätzungen, Datenschutz durch Technikgestaltung und Voreinstellung sollten gefördert und durch Material zur Bewusstseinsbildung unterstützt werden. Diese Vorgehnsweisen könnten durch Gesetze in bestimmten Rechtsbereichen vorgeschrieben werden.

Dienstleister für biometrische Authentifizierung, Software-Entwickler und Hardwarehersteller

30. Die Arbeitsgruppe fordert Dienstleister, Software-Entwickler und Hardwarehersteller nachdrücklich auf, sich über datenschutzfördernde Technologien im Bereich Biometrie zu informieren, sie zu implementieren und anzuwenden. Datenschutzbeauftragte und Datenschutzexperten sollten zu einem frühen Zeitpunkt bei Überlegungen zu biometrischen Lösungen eingebunden werden und Datenschutz-Folgeabschätzungen sollten an geeigneten Meilensteinen während der gesamten Lebensdauer des Projekts durchgeführt werden.

31. Falls biometrische Daten als Authentifizierungsfaktor genutzt werden, sollte dies nicht isoliert passieren, um ein angemessenes Niveau des Identitätsnachweises zur Verfügung zu stellen und die Risiken zu mindern, dass nicht autorisierte Dritte sich Zugang verschaffen.

32. Bei der Konzeption des biometrischen Authentifizierungssystems sollten die Organisationen Lösungen in Betracht ziehen, die die Speicherung der biometrischen Templates in zentralen Datenbanken und anderen Datendepots verhindern. Idealerweise sollte bei den Lösungen versucht werden, die biometrischen Templates lokal in einer sicheren Art und Weise zu speichern[21]

[21] Zum Beispiel als Hilfsdaten im Kontext der biometrischen Verschlüsselung oder als transformierte Daten im Kontext der widerrufbaren Biometrie.

(z. B. in einem gekapselten Speichergerät). Darüber hinaus ist es auch wichtig, dass die Authentifizierung lokal erfolgt, so dass keine biometrischen Daten (weder Sensor-Rohdaten noch Templates) das Computergerät verlassen.

33. Biometrische Systeme sollten so konzipiert sein, dass die biometrischen Rohdaten nach Generierung des biometrischen Template gesichert gelöscht werden können, es sei denn, dass sie wegen spezifischer und angemessener Gründe nicht gelöscht werden dürfen. Biometrische Templates (und die biometrischen Daten) müssen sicher gelöscht werden, wenn sie nicht länger benötigt werden (z. B. wenn der Nutzeraccount deaktiviert oder gelöscht wird). Hardwarehersteller sollten Möglichkeiten für eine sichere Löschung von biometrischen Templates zur Verfügung stellen und das biometrische Material in Endverbrauchergeräten verschlüsseln.

34. Nutzen Sie möglichst Systeme, die auf anerkannten Standards basieren. Standards werden typischerweise vielen Überprüfungen unterzogen und bieten zudem eine verbesserte Interoperabilität.

35. Die Dokumentation über relevante Hardware- und Softwarekomponenten sollte möglichst zur Verfügung gestellt werden. Dies gestattet es den Interessenvertretern in der Lieferkette, informierte Entscheidungen zu treffen und schneller zu reagieren, wenn Sicherheits- oder Datenschutzfehler entdeckt werden. Endverbraucher sollten in die Lage versetzt werden, informierte Datenschutz- und Sicherheitsrisikobewertungen zu machen.

36. Geeignete physikalische, technische und organisatorische Sicherheitsmaßnahmen, die auf dem neuesten Stand der Technik sind, müssen implementiert werden, um Schutz gegen Angriffe auf das System zu bieten. Bei der Speicherung biometrischer Templates sollten Organisationen die Nutzung spezialisierter Sicherheitsmodule[22] in Erwägung ziehen. Das reduziert die negativen Auswirkungen in dem Fall, dass das Hauptbetriebssystem erfolgreich angegriffen wurde. Effektiver Schutz gegen Spoofing und Fälschung der biometrischen Samples müssen ebenfalls vorhanden sein.

37. Dienstleister müssen standardmäßig die Menge der persönlichen Daten begrenzen, die gespeichert und während der Anmeldung und der Verifizierung der biometrischen Daten bearbeitet werden.

38. Dienstleister sollten ihre Kunden (d. h. die Organisationen, die das Authentifizierungssystem beschaffen) über den Datenschutz und die Sicherheits-

[22] Zum Beispiel die iOS Secure Enclave (https://support.apple.com/en-us/HT204587) oder das Android Trusted Execution Environment (https://source.android.com/security/authentication/fingerprint-hal.html)

charakteristika des biometrischen Authentifizierungsservices informieren, den sie nutzen. Diese Information sollte Einzelheiten über die Soft- und Hardwarehersteller, die vorhandenen Sicherheitsmaßnahmen, die Speichermodalitäten der biometrischen Daten, die Falschakzeptanzrate bzw. Falschrückweisungsrate sowie Angaben über die Aufbewahrungszeit biometrischer Daten enthalten.

39. Das biometrische System sollte so beschaffen sein, dass die Handlungen der Nutzer nicht durch die Anwendung verschiedener Implementationen eines biometrischen Authentifizierungssystems nachverfolgt werden können. Mit anderen Worten, das biometrische System muss die Unverkettbarkeit der gespeicherten Daten sicherstellen. Das bedeutet z. B., dass zwei Dienstleister, die biometrische Authentifizierungslösungen anbieten, nicht in der Lage sein dürfen, verschiedene Aktionen eines Anwenders durch die Anwendung der Authentifizierungstechnologie selbst zu korrelieren. Dies ist besonders wichtig, wenn ein Provider das gleiche System zwei oder mehreren unterschiedlichen Kunden anbietet.

40. Das biometrische System muss mit realistischen Testdaten, die auf die Situation angewendet werden, wo sie eingesetzt werden, getestet werden. Organisationen müssen sicherstellen, dass die Performanz und die Genauigkeitsgrade während der gesamten Lebensdauer des Systems angemessen sind.

Nutzerbeteiligung

41. Es müssen Systeme entwickelt werden, die dem Nutzer eine aktive Wahl bei der Authentifizierung mit Hilfe von Biometrie lassen und ihn nicht dazu zwingen, sie anzuwenden. Die Aufnahme in ein biometrisches Authentifizierungssystem muss stets ein bewusster Akt sein. Die Arbeitsgruppe fordert Dienstleister nachdrücklich dazu auf, ein alternatives (nicht-biometrisches) Authentifikationssystem für Anwender bereitzustellen, das ein angemessenes Sicherheitsniveau bietet. Man sollte außerdem beachten, dass es schwierig sein dürfte, eine rechtlich wirksame Einwilligung zu erhalten, falls keine praktikable Alternative zur Verfügung steht. Dies ist noch wichtiger, wenn die Einwilligung im Beschäftigungszusammenhang eingeholt werden soll.

42. Es sollte den Nutzern gestattet sein, den Dienstleister für ihre Authentifizierungstechnologie, wann immer dies möglich ist, auszuwählen. Dies gestattet es, sicherheitsbewussten Nutzern die standardbasierte Technologie ihrer Wahl auszuwählen und sie in kompatiblen Onlineservices wieder zu verwenden, ohne weitere finanzielle Ausgaben zu haben und ohne zusätzliche Hardware-Token mit sich herumzutragen.

Operationale Überlegungen

43. Alle Teilnehmer der Lieferkette müssen schnell auf Sicherheits- oder Datenschutzmängel in den Protokollen und der angewendeten Hardware oder Software reagieren.

44. Dienstleister müssen sicherstellen, dass Sicherheits- und Datenschutzfeatures ihrer Produkte standardmäßig aktiviert und Sicherheits- und Datenschutzmechanismen ohne überhöhte Kosten für den Kunden angeboten werden.

45. Dienstleister sollten föderierten Zugriff auf ihre Dienste anbieten, da individuelle Registrierungsprozesse zeitaufwändiger sein könnten, wenn biometrische Profile generiert werden müssen. Dies gestattet es den Anwendern, ihren existierenden Identitätsprovider weiterzunutzen, ohne sich bei jeder Site registrieren zu müssen. Föderierte Identitätsprovider müssen jedoch die Notwendigkeit respektieren, den Umfang und die Verkettbarkeit der Daten, die sie speichern, zu begrenzen.

Anwender

46. Nutzer von biometrischen Dienstleistungen sollten die mögliche Gefährdung des Datenschutzes und den Schutz der Privatsphäre bei der Verwendung biometrischer Authentifizierung ernst nehmen, die ihnen von Seiten des Dienstleisters übermittelt wurden. Sie sollten sich auch über die Sicherheits- und Datenschutzeigenschaften der verschiedenen Dienstleister informieren und die Dienstleistungen und Dienstleister, die sie nutzen, entsprechend auswählen. Schließlich sollten sie sich vergewissern, dass die existierenden Sicherheits- und Datenschutzfeatures einer Dienstleistung aktiviert sind, bevor sie den Service nutzen, und sich einen alternativen Mechanismus statt einer biometrischen Authentifizierung zunutze machen, falls sie dies wünschen.

B. Dokumente zur Informationsfreiheit

I. Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließung zwischen der 30. und der 31. Konferenz (vom 28. April 2016)

Auch die Verwaltungen der Landesparlamente sollen Gutachten der Wissenschaftlichen Dienste proaktiv veröffentlichen!

Nach der aktuellen Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 25. Juni 2015, Az.: 7 C 1/14) muss die Bundestagsverwaltung auf Antrag Zugang zu den Ausarbeitungen der Wissenschaftlichen Dienste gewähren.

Wie der Deutsche Bundestag inzwischen bekannt gab, bedarf es derartiger individueller Anträge seit dem 18. Februar 2016 nicht mehr, denn die Bundestagsverwaltung veröffentlicht generell die Ausarbeitungen der Wissenschaftlichen Dienste nunmehr vier Wochen nach Auslieferung an die auftraggebenden Abgeordneten, damit diese zunächst die Möglichkeit haben, die Gutachten exklusiv nutzen zu können, proaktiv im Internet. Dabei werden die Namen der Auftraggeber nicht bekannt gegeben.

Die Entscheidung zur proaktiven Veröffentlichung ist im Sinne von Open Data und Transparenz nachdrücklich zu unterstützen, da es ein großes öffentliches Interesse an den Ausarbeitungen der Wissenschaftlichen Dienste gibt. So lagen infolge der neuen Rechtsprechung des Bundesverwaltungsgerichts der Bundestagsverwaltung in kürzester Zeit weit über 2000 Informationszugangsanträge vor. Die individuelle Bearbeitung dieser Anträge hätte in aller Regel viel Zeit gebunden und unnötig hohe Personal- und Sachkosten verursacht. Durch die Entscheidung werden die Kosten sowohl für die Verwaltung als auch für die Bürgerinnen und Bürger deutlich gesenkt. Die Ausarbeitungen stehen der interessierten Öffentlichkeit zukünftig schnell und einfach zur Verfügung.

Vor diesem Hintergrund fordert die Konferenz der Informationsfreiheitsbeauftragten in Deutschland die Verwaltungen der Landesparlamente auf, dem Beispiel der Bundestagsverwaltung in Sachen Transparenz und Open Data zu folgen. Dabei sind etwaige Ausschlussgründe (insbesondere durch Schwärzung der Namen

der Auftraggeber) sowie landesrechtliche Vorgaben zu berücksichtigen. Auch die Verwaltungen der Landesparlamente sollten Ausarbeitungen der jeweiligen Wissenschaftlichen Dienste bzw. der Gesetzgebungs- und Beratungsdienste unabhängig von individuellen Zugangsanträgen im Internet veröffentlichen, soweit dies nicht bereits geschieht.

2. Entschließung der 31. Konferenz am 15. Juni 2016 in Düsseldorf

GovData: Alle Länder sollen der Verwaltungsvereinbarung beitreten und Daten auf dem Portal bereitstellen!

„GovData – das Datenportal für Deutschland“ ist eine Anwendung des IT-Planungsrats, die auf der Grundlage einer Verwaltungsvereinbarung vom Bund und mehreren Ländern betrieben wird. Das Portal bietet einen einheitlichen zentralen Zugang zu offenen Verwaltungsdaten aus Bund, Ländern und Kommunen. Ziel ist es, diese Daten möglichst flächendeckend zur Verfügung zu stellen und sie an einer zentralen Stelle auffindbar und so einfacher nutzbar zu machen. GovData dient damit nicht nur der Information der Bürgerinnen und Bürger, sondern fördert zugleich auch die Transparenz und Akzeptanz des Verwaltungshandelns. Es stellt der Wirtschaft darüber hinaus Verwaltungsdaten zur Entwicklung neuer Geschäftsmodelle zur Verfügung.

Bislang beteiligen sich jedoch an dem Bund-Länder-Online-Portal noch nicht alle Länder. Viele Daten, an deren Veröffentlichung ein großes öffentliches Interesse besteht, sind noch nicht abrufbar. Das immense wirtschaftliche Potential von Open Data bleibt ungenutzt.

Sowohl für die Wirtschaft als auch für die Zivilgesellschaft ergeben sich erhebliche Vorteile durch einen freien Zugang zu den öffentlichen Daten der Verwaltung. Der Umfang und die Qualität der in GovData zur Verfügung gestellten Daten müssen verbessert und der Nutzwert des Portals weiter erhöht werden.

Daher appelliert die Konferenz der Informationsfreiheitsbeauftragten in Deutschland an die verbleibenden Länder, der Verwaltungsvereinbarung beizutreten, und fordert alle Vereinbarungspartner zur verstärkten Bereitstellung von Daten auf.

3. Entschließung der 32. Konferenz am 2. Dezember 2016 in Düsseldorf

Nicht bei Open Data stehenbleiben: Jetzt auch Transparenzgesetze in Bund und Ländern schaffen!

Entschließung der Informationsfreiheitsbeauftragten[1]

Die Konferenz der Informationsfreiheitsbeauftragten fordert die Gesetzgeber in Bund und Ländern auf, jetzt flächendeckend Transparenzgesetze zu schaffen. Solche Gesetze verbinden den individuellen, antragsgebundenen Informationszugangsanspruch mit der Verpflichtung öffentlicher Stellen, bestimmte Informationen aktiv auf Informationsplattformen im Internet zu veröffentlichen.

Anlass für die Forderung ist ein Beschluss der Regierungschefs von Bund und Ländern vom 14. Oktober 2016. Nach dieser Vereinbarung werden Bund und Länder Open-Data-Gesetze erlassen und das Ziel verfolgen, bundesweit vergleichbare Standards für den Zugang zu öffentlichen Datenpools zu erreichen.

Die Informationsfreiheitsbeauftragten befürworten zwar die Zielrichtung des Beschlusses; dieser greift jedoch zu kurz. Neben der Bereitstellung von Rohdaten in standardisierten und offenen Formaten für eine Weiterverwendung gebietet die Transparenz öffentlichen Handelns, zusammenhängende, aus sich heraus nachvollziehbare Unterlagen zur Verfügung zu stellen. Hierfür kommen beispielsweise Verträge, Gutachten, Studien, umweltrelevante Konzepte, Pläne, Programme oder Zulassungsentscheidungen, Berichte, Protokolle, Beschlüsse, Organisationserlasse, Statistiken, öffentliche Planungen, Haushalts-, Stellen-, Organisations-, Geschäftsverteilungs- und Aktenpläne, Drucksachen, Verwaltungsvorschriften oder wesentliche Bestandteile von Subventions- und Zuwendungsvergaben und Baugenehmigungen sowie die wesentlichen Unternehmensdaten öffentlicher Beteiligungen einschließlich der Vergütung der Leitungsebenen infrage.

Daher fordert die Konferenz, dass Bund und Länder ihre Behörden verpflichten, derartige Dokumente grundsätzlich im Internet zu veröffentlichen. Der bekannt gewordene Entwurf des Eckpunktepapiers des Bundes vom 18.10.2016[2] genügt diesen Anforderungen nicht. Anstatt separate Gesetze zu schaffen oder die Regelungen den eher informationstechnisch orientierten E-Government-Gesetzen zu überlassen, sollte der Beschluss der Regierungschefs von Bund und Ländern so umgesetzt werden, dass Open-Data-Regelungen in Transparenzgesetze aufgenommen werden. Länder, die noch nicht über solche Gesetze verfügen, sollten

[1] Bei Enthaltung des Bundes

[2] Siehe netzpolitik.org

nach Auffassung der Informationsfreiheitsbeauftragten vorhandene Informationsfreiheitsgesetze entsprechend fortentwickeln. Auch fordert die Konferenz jene Länder auf, die keinen allgemeinen Anspruch auf Informationszugang gewähren, endlich ein modernes Informationsrecht einzuführen.

Der vorliegende Band mit Dokumenten aus dem Jahr 2016 enthält:

Beschlüsse, Entschließungen sowie Arbeitspapiere der nationalen und internationalen Arbeitsgruppen und Konferenzen zum Datenschutz und zur Informationsfreiheit.

www.datenschutz-berlin.de

Berlin