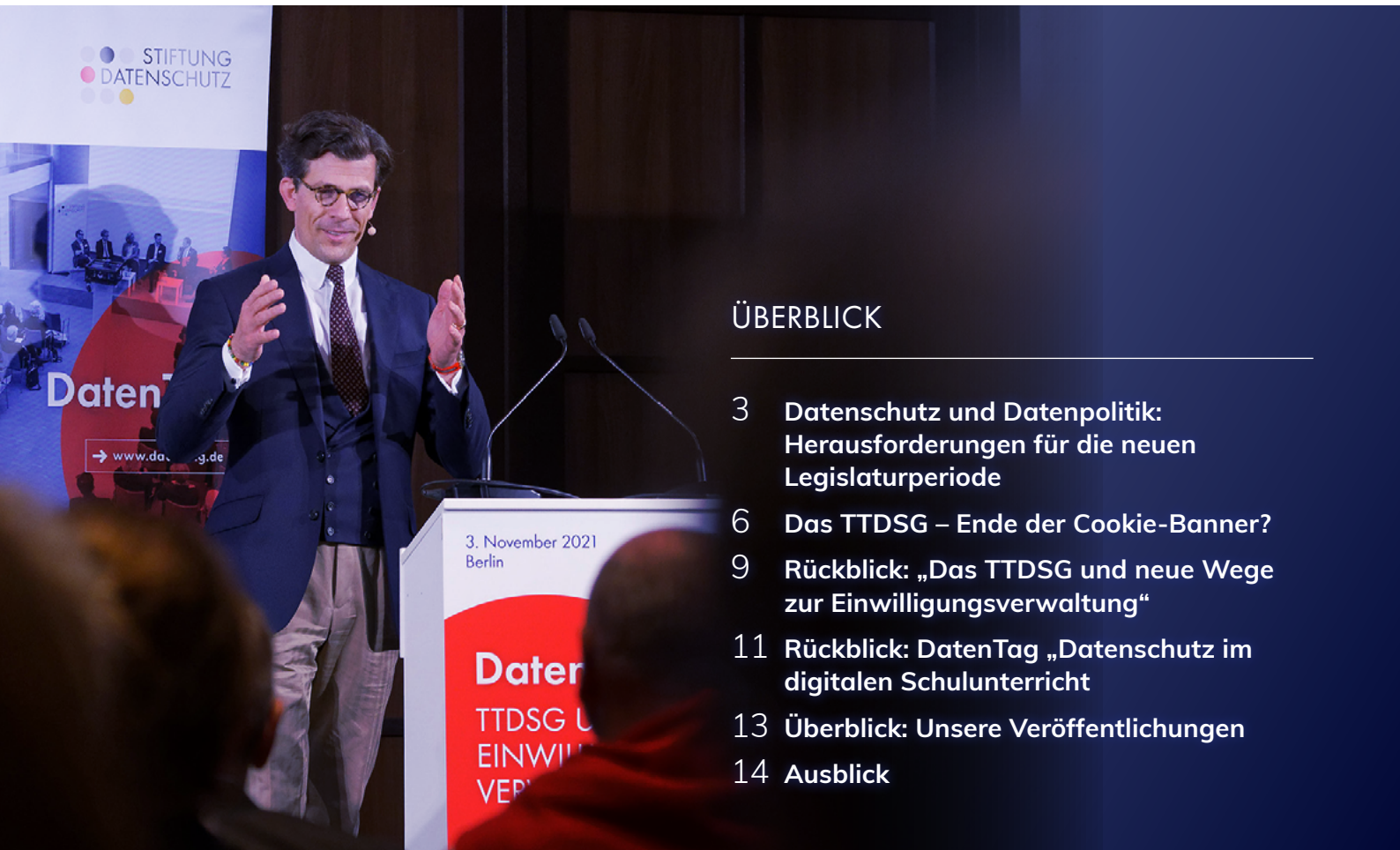
STIFTUNG DATENSCHUTZ

POLITIKBRIEF – HERBST/WINTER 2021

DATENSCHUTZ IN DER NEUEN LEGISLATURPERIODE



ÜBERBLICK

3 Datenschutz und Datenpolitik: Herausforderungen für die neuen Legislaturperiode

6 Das TTDSG – Ende der Cookie-Banner?

9 Rückblick: „Das TTDSG und neue Wege zur Einwilligungsverwaltung“

11 Rückblick: DatenTag „Datenschutz im digitalen Schulunterricht

13 Überblick: Unsere Veröffentlichungen

14 Ausblick

Liebe Leserinnen und Leser,

die alte Bundesregierung hatte wenige Monate vor Ende der Wahlperiode ihre Datenstrategie vorgestellt. Noch ist unklar, welche Prioritäten die neue Regierung in der Datenpolitik setzen wird.

Aus unserer Sicht sollte vor allem die zu Recht in der Datenstrategie herausgehobene Forderung nach mehr Datenkompetenz weiterverfolgt werden. Auch die beabsichtigte Ausweitung von Datenzugang und Datennutzung würde der Allgemeinheit nutzen – aber gleichzeitig erfordern dies Wissen um eine rechtssichere Datenverarbeitung. Datennutzungskompetenz und Datenschutz müssen daher Hand in Hand gehen. Unsere Empfehlungen zu Datenschutz und Datenpolitik finden Sie auf den nächsten Seiten.

Aus aktuellem Anlass erläutert Prof. Dr. Anne Riechert das „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG), das am 1. Dezember in Kraft treten wird. Auf unserer Konferenz am 3. November wurde das Thema umfassend und lebhaft diskutiert.

Wir berichten außerdem von unserer Online-Konferenz zum Datenschutz im digitalen Unterricht und geben einen Überblick über unsere Publikationen.

Herzlich grüßt

Frederick Richter, Vorstand der Stiftung Datenschutz

DATENSCHUTZ UND DATENPOLITIK: HERAUSFORDERUNGEN FÜR DIE NEUEN LEGISLATURPERIODE

Das Ziel moderner Daten- und Digitalpolitik sollte es sein, die Nutzung von Daten zum Wohle der Allgemeinheit zu fördern. Gleichzeitig sind die Rechte und Freiheiten der Menschen wirksam zu schützen. Für das Vertrauen in die Digitalisierung sind daher zwei Dinge unverzichtbar: Gute IT-Sicherheit zum technischen Schutz von Daten und guter Datenschutz zur Wahrung der Grundrechte.

Der Beginn der neuen Wahlperiode bietet die Chance für neue Initiativen zur Regulierung des Umgangs mit Daten. Manche Vorhaben können bereits auf nationaler Ebene angegangen werden. Bei europäischer Zuständigkeit kann die neue Bundesregierung auf Reformen hinwirken und Impulse geben. Die lange Tradition Deutschlands in der Datenschutzgesetzgebung lässt sich mit Vorschlägen zu innovativer Datenpolitik schlüssig fortsetzen.

DIE BUNDESSTIFTUNG WILL DAZU AKTIV BEITRAGEN

Aus Sicht der Stiftung Datenschutz sollten die folgenden Punkte im Vordergrund stehen:

- Die Förderung von **Wissen** über den verantwortungsbewussten und datenschutzkonformen Umgang mit personenbezogenen Daten
- Die Entwicklung von **Leitlinien zur Anonymisierung**, um breitere Datennutzung zu ermöglichen
- Die Förderung von **Datentreuhandstrukturen**, um das Teilen und Nutzen von personenbezogenen Daten zu erleichtern
- Die **Vereinheitlichung der Datenschutzaufsicht** für die konsistente Rechtsanwendung und **Arbeitsteilung** für mehr Effizienz
- Regelungen zum **Beschäftigtendatenschutz** für mehr Rechtssicherheit im Arbeitsverhältnis
- Förderung von Werkzeugen zum **Einwilligungsmanagement / PIMS** für mehr Nutzersouveränität

DIE EMPFEHLUNGEN IM EINZELNEN

Förderung von mehr Datenkompetenz und Verbreitung von Datenschutzwissen

Datenschutz ist komplex und muss erklärt werden. Diese Herausforderung betrifft alle Sektoren, denn die nicht immer einfachen Anforderungen müssen überall beachtet werden: In Unternehmen, Vereinen und anderen Organisationen, egal ob öffentlich-rechtlich oder privatrechtlich organisiert und völlig unabhängig von der Größe.

Mehr Datennutzung durch Rechtssicherheit bei der Anonymisierung

Die praktische Bedeutung der Anonymisierung von personenbezogenen Daten ist sehr hoch. Mit der Entfernung des Personenbezuges wird der Geltungsbereich des Datenschutzrechts komplett verlassen, und es bieten sich für die

„entschärften“ Datensätze deutlich weitere Einsatzmöglichkeiten. Daten können zum Wohle der Allgemeinheit und zur Wertschöpfung genutzt werden, z.B. als Trainingsdaten für Systeme maschinellen Lernens und künstlicher Intelligenz. Dennoch ist der entscheidende Vorgang des Anonymisierens gesetzlich nicht geregelt und es bestehen Unsicherheiten. Als Folge dessen werden Potentiale von Daten oft nicht ausgeschöpft und wird das Instrument der Anonymisierung weniger genutzt. Dies ist nicht im Sinne von Wirtschaft und Entwicklung und ebenso nicht im Sinne des Datenschutzes als Bürgerrecht.

In der DSGVO werden anonyme und anonymisierte Daten bislang allein im Erwägungsgrund 26 erwähnt. Das Gesetz legt nicht fest, wann eine Anonymisierung als belastbar genug angesehen werden kann, um den Schutzbereich der DSGVO zu verlassen. Für die Anonymisierung braucht es daher Leitlinien für eine gute und handhabbare Datenschutzpraxis. Mit einer solchen Richtschnur kann Orientierung geschaffen und Rechtssicherheit gefördert werden.

Aufbau von Datentreuhandstrukturen

Die Frage des Zugangs zu Daten wird immer mehr in den Vordergrund rücken. Zukünftig wird es weniger darum gehen, wem Daten „gehören“, sondern vielmehr darum, wer welche Daten nutzen darf.

Treuhandmodelle können das freiwillige Teilen von Daten und die Nutzung durch Dritte über eine neutrale Instanz erleichtern. Der Aufbau von Treuhandstrukturen für die Verwaltung von Datenzugangsrechten kann bei personenbezogenen Daten auch die Datenkontrolle und -souveränität der betroffenen Personen stärken. Notwendig ist für jede dieser möglichen Aufgaben eine unabhängige und vertrauenswürdige Einrichtung.

> Damit das einheitliche europäische Datenschutzrecht seine volle Wirkung entfalten kann, muss das Recht einheitlich angewendet werden. Das erfordert weitestgehende Einigkeit unter den Aufsichtsbehörden.
> **Prof. Dr. Anne Riechert, Wissenschaftliche Leiterin der Stiftung Datenschutz**

Effizientere Datenschutzdurchsetzung durch Vereinheitlichung und bessere Ausstattung der Datenschutzaufsicht:

Die Einigkeit unter den Aufsichtsbehörden wird im föderal organisierten Deutschland nicht immer erreicht; unterschiedliche Auslegungen des harmonisierten europäischen Datenschutzrechts vergrößern ohne Not Rechtsunsicherheiten. Da sich jedoch zeigt, dass sich eine einheitliche Sicht von alleine nicht einstellt, sollte die neue Bundesregierung eine Reform angehen. Dazu sind die bestehenden Vorschläge für verbindliche Beschlüsse der Konferenz der deutschen Aufsichtsbehörden und für kurze Fristen zu gemeinsamen Entscheidungen aufzugreifen. Die DSGVO mit ihrem funktionierenden Kohärenzmechanismus kann dabei Vorbild sein.

WAS DIE STIFTUNG BEITRAGEN KANN

Die Stiftung Datenschutz verfügt über umfassende Expertise zu den genannten Themen, die sich in zahlreichen Veröffentlichungen und Veranstaltungen widerspiegelt. Das Stiftungshandeln ist unabhängig und frei von gewerblichen oder politischen Interessen. Damit ist die Stiftung besonders geeignet als neutrale Plattform für Diskussionen zu aktuellen Themen, aber auch für die sachkundige Beratung bei der Entwicklung von Gesetzen und Richtlinien.

Im Rahmen einer stärker arbeitsteiligen Vorgehensweise der deutschen Datenschutzbehörden können die vorhandenen Kapazitäten besser genutzt werden. Während alle Behörden für die Überwachung der DSGVO-Konformität in ihrem jeweiligen räumlichen Zuständigkeitsbereich generell verantwortlich bleiben, sollten spezielle Themen federführenden Aufsichten zugewiesen werden (Bildung, Zertifizierung, Gesundheitsdatenschutz u.ä.).

Mehr Rechtsklarheit durch spezielle Regelungen zum Beschäftigtendatenschutz

Es sollte mehr Rechtssicherheit beim Datenschutz für Beschäftigtendaten geben. An dieser Stelle kann der Gesetzgeber selber Rechtsverbindlichkeit schaffen und muss diese wichtige Aufgabe nicht weiter den Arbeitsgerichten überlassen. Dies gilt gerade angesichts des Spielraumes, den die DSGVO den Mitgliedstaaten bei diesem Thema – anders als in vielen anderen Punkten – lässt.

Für Beschäftigte ist oftmals nicht klar, unter welchen Voraussetzungen die Verarbeitung der sie betreffenden Daten rechtmäßig ist. Offen ist auch die Reichweite heimlicher Überwachung oder heimlicher Kontrollen von Beschäftigten. Umstritten ist zudem, inwieweit Arbeitgeber im Rahmen der Durchführung des Beschäftigungsverhältnisses eine Datenverarbeitung auf ihre berechtigten Interessen als Rechtsgrundlage stützen können. Auch neue Technologien, insbesondere die Möglichkeiten von Systemen künstlicher Intelligenz, sollten dabei berücksichtigt werden.

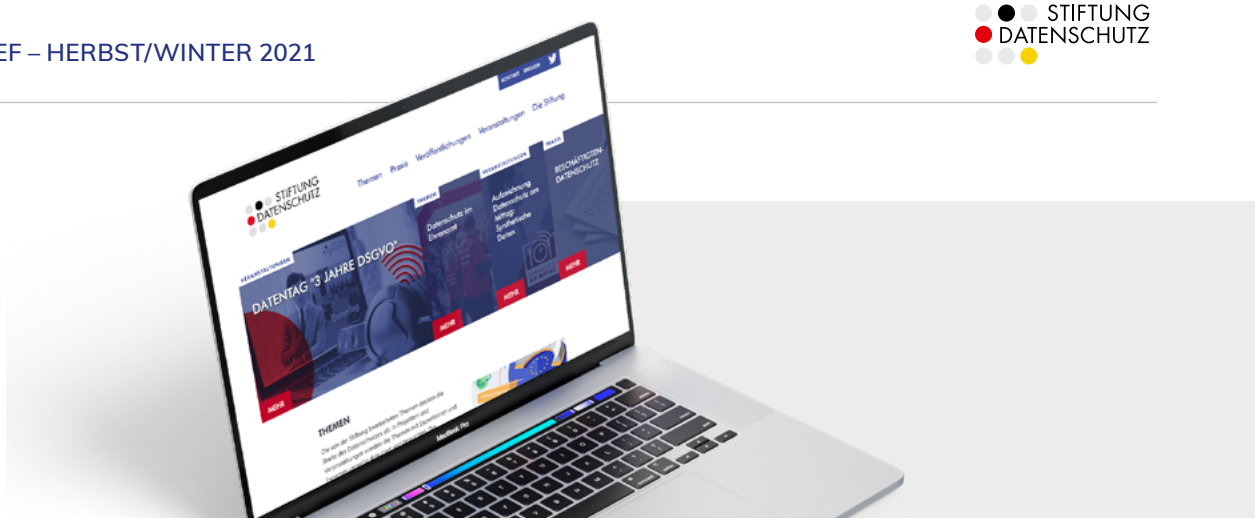
Stärkung der Nutzersouveränität durch Förderung von Einwilligungsmanagement

Die Auseinandersetzung mit „Personal Information Management Services“ (PIMS) befindet sich in Deutschland noch am Anfang. Für mehr Datennutzungskontrolle sollen PIMS-Systeme es ermöglichen, im Rahmen eines Einwilligungsmanagements Dritten den Zugriff auf persönliche Daten gezielter zu gestatten oder zu verweigern.

Auf der anderen Seite können PIMS-Dienste den Unternehmen den von ihnen geschuldeten Nachweis datenschutzrechtlicher Einwilligungen erleichtern, was den Dokumentationsaufwand mindert und die Rechtssicherheit steigert.

Gegenüber Wirtschaftsakteuren als Datennehmern sollen PIMS den Menschen als Datengebern auch zu mehr Verhandlungsmacht verhelfen und damit Machtungleichgewichte und Informationsasymmetrien mindern.

Im Rahmen der im neuen Jahr zu erlassenden Rechtsverordnung zu § 26 TTDSG sollte die neue Bundesregierung zu PIMS wegweisende Festlegungen treffen.



DAS TTDSG – ENDE DER COOKIE-BANNER?

Im Mai 2021 hat der Bundestag das „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“ beschlossen. Das Telekommunikation-Telemedien-Datenschutzgesetz, kurz: TTDSG, tritt am 01. Dezember in Kraft – zeitgleich mit einem modernisierten Telekommunikationsgesetz (TKG). Die Vorschriften zum Datenschutz in der Telekommunikation und bei Telemedien werden nun in einem einheitlichen Gesetz zusammengefasst.

WARUM?

Es bestand Anpassungsbedarf der Datenschutzbestimmungen im Telemediengesetz (TMG) und im Telekommunikationsgesetz (TKG) an die Datenschutzgrundverordnung sowie an die europäische ePrivacy-Richtlinie (Richtlinie 2002/58/EG, geändert durch die Richtlinie 2009/136/EG). Nach dem Willen des Gesetzgebers sollen damit auch Unklarheiten für Verbraucher und Dienstanbieter beseitigt werden und es werden aus datenschutzrechtlicher Sicht obsolete Vorschriften des TKG und des TMG aufgehoben. Ebenso wird nun eindeutig geklärt, dass auch Messengerdienste wie WhatsApp oder webgestützte E-Mail-Dienste als Telekommunikationsdienste einzustufen sind. Denn während Beispiele für Telemediendienste regelmäßig präzise benannt werden konnten und können (Webseiten, Onlineshops, Angebot von Wetter-, Verkehrs-, Börsendaten, On-Demand-Dienste, etc.), war die Einordnung von solchen „neuen“ Internetdiensten umstritten. Als „nummernunabhängige interpersonelle Kommunikationsdienste“, sogenannte „Over-the-top-(OTT)-Dienste“ ordnete der Europäische Gerichtshof - anders als die Bundesnetzagentur – diese nicht als Telekommunikationsdienste ein. Die nun erfolgte Klarstellung ist allerdings nicht unmittelbar den datenschutzrechtlichen Regelungen im TTDSG zu entnehmen, sondern dem modernisierten Telekommunikationsgesetz, welches den europäischen Kodex für die elektronische Kommunikation (Kodexrichtlinie 2018/1972) umsetzt. Das TTDSG verweist aber auf diese neuen Bestimmungen.

WAS IST NEU?

Neu sind Bestimmungen zum Schutz der Privatsphäre bei Endeinrichtungen. Diese dienen der Umsetzung der europäischen ePrivacy-Richtlinie, der so genannten Cookie-Richtlinie, die weiterhin in Kraft ist: Die Speicherung von oder der Zugriff auf Informationen in einem Endgerät ist nur auf der Grundlage einer Einwilligung möglich. Hierzu hatte der Bundesgerichtshof in der Vergangenheit bereits ein Urteil gefällt und entschieden, dass ein Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder der Marktforschung nur mit Einwilligung des Nutzers einsetzen darf. Adressaten dieser Regelung sind in erster

Linie Anbieter von Telemedien, da sie für die Nutzerinnen und Nutzer Inhalte bereitstellen und somit leicht auf deren Endgeräte zugreifen können. Zu berücksichtigen ist jedoch, dass die entsprechende Regelung im TTDSG offen formuliert ist: Niemand darf Informationen in der Endeinrichtung des Endnutzers speichern oder auf gespeicherte Informationen zugreifen. Die Vorschrift beinhaltet daher ein allgemeines Verbot.

Ebenso neu und daran anknüpfend sind Regelungen zur Verwaltung und Einholung von Einwilligungen. Diesen Themenkomplex der „Personal Information Management Systeme“ (PIMS) hat die Stiftung Datenschutz mit Fokus auf die technischen, rechtlichen und ökonomischen Herausforderungen schon in den Jahren 2016/2017 aufgegriffen und eine Studie mit dem Titel „Neue Wege bei der Einwilligung“ erstellt[1] . Im November 2021 diskutierten wir anlässlich des bevorstehenden Inkrafttretens des TTDSG ausführlich auf einer Fachkonferenz[2].

Neu im TTDSG ist auch, dass Telekommunikationsunternehmen einer einheitlichen Datenschutzaufsicht durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterworfen werden, d.h. gleichermaßen im Hinblick auf den Schutz der Privatsphäre bei Endeinrichtungen: Ruft ein Nutzer oder eine Nutzerin die Webseite eines Anbieters eines Telekommunikationsdienstes auf, regelt das TTDSG nun eindeutig, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als unabhängige Datenschutzaufsichtsbehörde zuständig ist.

Neu ist schließlich die gesetzliche Regelung, dass der Zugriff auf Daten eines verstorbenen Endnutzers beim Telekommunikationsunternehmen möglich ist und das Fernmeldegeheimnis dem nicht entgegensteht. Bereits in der Vergangenheit hatte der Bundesgerichtshof hierzu entschieden, dass Facebook den Erben den Zugang zu dem Benutzerkonto und den darin vorgehaltenen Kommunikationsinhalten beim Tod des Kontoinhabers ermöglichen muss.

ENDLICH RECHTSKLARHEIT?

Datenschutzrechtliche Regelungen für Anbieter von Telekommunikationsdiensten, die bereits im TKG a.F. geregelt waren, werden weitgehend unverändert übernommen und stellen im Kern keine neuen materiellen Vorschriften dar. Problematisch ist dies, da manche dieser Regelungen bereits in der alten Fassung des TKG von der ePrivacy-Richtlinie abwichen und jede Abweichung von den Regelungen der ePrivacy-Richtlinie Abweichung die Gefahr der Europarechtswidrigkeit beinhaltet

Auch bestimmte „alte“ Streitfragen werden nicht gelöst, etwa inwieweit der Arbeitgeber Anbieter eines Telekommunikationsdienstes sein kann und zur Einhaltung des Fernmeldegeheimnisses verpflichtet ist. So sollen gemäß des TTDSG Anbieter von „geschäftsmäßig“ angebotenen Telekommunikationsdiensten zur Wahrung des Fernmeldegeheimnisses verpflichtet sein. Umstritten war je-doch stets, ob davon Arbeitgeber umfasst sind. Dies wird auch durch das TTDSG nicht beantwortet und den Begriff der „Geschäftsmäßigkeit“ kennt die ePrivacy-Richtlinie nicht.

Die Einwilligungsregelung des TTDSG lässt ebenfalls Fragen offen. Zwar wird die Notwendigkeit einer Einwilligung gesetzlich geregelt und gemäß den europäischen Vorgaben umgesetzt, wenn Informationen in der Endeinrichtung des Endnutzers gespeichert werden oder der Zugriff auf gespeicherte Informationen erfolgt. In der Literatur wird aber beispielsweise diskutiert, ob die entsprechende Regelung im TTDSG technologieneutral ist. Thematisiert wird ebenso, inwieweit hiervon beispielsweise eigene Messungen der Zugriffszahlen auf Webseiten erfasst sind, da diese nicht unbedingt erforderlich sind. Die Messung von Zugriffszahlen auf Webseiten wird von der ePrivacy-Richtlinie nicht geregelt und eine abweichende Vorschrift im TTDSG wäre damit ohnehin europarechtswidrig erfolgt. Ein nationaler Gesetzgeber ist in seinem Spielraum bei der Umsetzung der aktuell geltenden ePrivacy-Richtlinie eingeschränkt.

1 *https://sds-links.de/einwilligung*
2 *https://sds-links.de/TTDSG*

Diesbezüglich könnte nur die auf europäischer Ebene geplante ePrivacy-Verordnung Rechtssicherheit schaffen und Unklarheiten beseitigen. So wurde beispielsweise die Reichweitenmessung von Webseiten bereits im ersten Entwurf der EU-Kommission zur ePrivacy-Verordnung privilegiert und in den Entwürfen der unterschiedlichen Ratspräsidentschaften sogar erweitert, u.a. auf Zwecke der Betrugsprävention oder zum Zwecke von Softwareupdates. Unabhängig von der politischen und rechtlichen Würdigung solcher Zwecke im Einzelfall kann eine Verordnung auf europäischer Ebene solche Fallgestaltungen grundsätzlich regeln. Derzeit stehen etwa auf der Webseite des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg Informationen über die datenschutzgerechte Vorgehensweise einer Reichweitenanalyse zum Abruf bereit[3].

Auch mit Blick auf die „Dienste zur Einwilligungsverwaltung“ braucht es noch Antworten. Diskutiert werden beispielsweise die Fragen nach einer Stellvertretung bei der Einwilligung, nach der technischen Ausgestaltung und möglicher technischer Hürden solcher Dienste oder nach der praktischen Ausgestaltung vor dem Hintergrund der engen Zweckbindung der DS-GVO. Im Übrigen enthält auch der Vorschlag für eine ePrivacy-Verordnung die Möglichkeit, die Einwilligung mittels technischer Einstellungen einer Software zu erteilen. Im ersten Entwurf der Kommission war sogar (bußgeldbewehrt) geregelt, dass die Software bei der Installation über die Einstellungsmöglichkeiten zur Privatsphäre informieren und die Einwilligung zu einer Einstellung des Endnutzers verlangen muss. Letzteres wurde jedoch in den nachfolgenden Entwürfen der unterschiedlichen Ratspräsidentschaften gestrichen. In diesem Zusammenhang ist außerdem eine weitere, auf europäischer Ebene geplante Verordnung (Data Governance Act) zu berücksichtigen, die umfassende Regelungen zu „Data Sharing Services“ (Datenvermittler) enthält. Die Regelung im TTDSG könnte jedoch für Auslegungsfragen rund um die Ausgestaltung von „Personal Information Management Systemen“ (PIMS) eine Vorreiterrolle einnehmen, da nun in einer Rechtsverordnung die Fragen und Anforderungen an das Verfahren geklärt und näher bestimmt werden müssen, die auch auf europäischer Ebene relevant sein können. Dennoch kann natürlich bei Inkrafttreten des Data Governance Act die Interpretation eines „Dienstes zur Einwilligungsverwaltung“ auf nationaler Ebene nur insofern eine Rolle spielen, wie sie einer europaweiten Harmonisierung nicht zuwiderläuft. Die Auslegung hat stets im europäischen Kontext zu erfolgen und letztendlich ist auch eine Regulierung von Datenintermediären und eine PIMS-Reglung nur auf einer europäischen Ebene sinnvoll.

FAZIT

Das Nebeneinander der datenschutzrechtlichen Vorschriften führte vor allem bei Verbraucher:innen und Diensteanbietern zu Unsicherheiten, die nun durch das TTDSG beseitigt werden. Rechtliche Unklarheiten bleiben jedoch auch nach Inkrafttreten des TTDSG bestehen und es werden sogar bei einzelnen Regelungen Zweifel an der Vereinbarkeit mit dem EU-Recht geäußert. Rechtsklarheit könnte mit der europaweit geltenden ePrivacy-Verordnung geschaffen werden – vorausgesetzt die Mitgliedstaaten einigen sich auf eine solche. Außerdem ist der Vorschlag der Europäischen Kommission zum geplanten Data Governance Act im Blick zu behalten, der eine europaweite Harmonisierung für eine gemeinsame Datennutzung schaffen möchte und damit über die Einwilligungsverwaltung im TTDSG hinausgeht.

3 https://www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2/

RÜCKBLICK: „DAS TTDSG UND NEUE WEGE ZUR EINWILLIGUNGSVERWALTUNG“

Anfang Dezember tritt das Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) in Kraft. Es setzt die ePrivacy-Richtlinie um und reguliert vor allem das Nutzertracking zu Werbezwecken.

Wir haben Expertinnen und Experten in die Historische Kassenhalle des Humboldt Carré geladen, um die unterschiedlichen Sichtweisen und Erwartungen zu diskutieren.

STAND DES VERFAHRENS

Thomas Jarzombek, MdB, Beauftragter des Bundesministeriums für Wirtschaft und Energie für die Digitale Wirtschaft und Startups, forderte einen pragmatischen Datenschutz, der funktioniert. Personal Information Management Services (PIMS) seien eine vielversprechende Möglichkeit, die eigenen Präferenzen an Website-Betreiber zu übermitteln. Auch sogenannte Datentreuhänder, die ohne eigenes wirtschaftliches Interesse personenbezogene Daten verwalten und zugänglich machen, sollten in Zukunft an Bedeutung gewinnen.

Im Bundeswirtschaftsministerium wird derzeit an einer Verordnung gearbeitet, die Nutzer:innen mehr Kontrolle über die Verwendung ihrer Daten geben soll. Dazu wird gerade ein Gutachten erstellt, an dem Stefan Weiß von der Gesellschaft für Datenschutz und Datensicherheit, Christiane Wendehorst von der Universität Wien und weitere Autor:innen schreiben. Wenn alles läuft wie geplant, könnte die Verordnung Ende des kommenden Jahres in Kraft treten, so der zuständige Referatsleiter Rolf Bender.

Weiß und Wendehorst schalteten sich im Verlauf der Veranstaltung zu, um einen Überblick über den Stand der Dinge zu geben und sich an der Diskussion zu beteiligen.

DAS ENDE DER EINWILLIGUNG?

Viele Vorträge und Debatten drehten sich um die Einwilligung in die Datenverarbeitung, die sich oft nur in einem Klick auf die allseits unbeliebten „Cookie-Banner“ ausdrückt. Scharf kritisiert wurde das bestehende System der Einwilligung von Malte Engeler, Richter am Schleswig-Hosteinischen Verwaltungsgericht und Datenschutzexperte. Der Gesetzgeber sollte verhindern, dass die Einwilligung als Rechtsgrundlage „toxische Geschäftsmodelle“ ermögliche. Kristin Benedikt, Richterin am Verwaltungsgericht Regensburg und ehemals bei der bayerischen Aufsichtsbehörde hauptberuflich mit der Materie befasst, hält PIMs, wenn sei gut umgesetzt seien, für eine sinnvolle Lösung des Einwilligungsdilemmas, denn schon jetzt ermögliche die DSGVO die Datenverarbeitung auf Basis anderer Rechtsgrundlagen, die nur zu selten genutzt würden.

Ganz konkrete Lösungen für die Verwaltung personenbezogener Daten stellen Achim Schlosser von Net-ID und Max Schrems von der österreichischen Bürgerrechtsorganisation NOYB vor. Louisa Specht-Riemenschneider von der Forschungsstelle Datenrecht der Universität Bonn zeigte die Potentiale der Datentreuhänder auf.

UNTERSCHIEDLICHE INTERESSEN: WIRTSCHAFT UND VERBRAUCHER

Für die datenverarbeitende (Werbe-)Wirtschaft diskutierten Michael Neuber von Google, Bernd Nauen vom Zentralverband der Werbewirtschaft und Christian Dürschmied vom Branchenverband der digitalen Wirtschaft. Dabei traten ganz unterschiedliche Sichtweisen zutage: Während Google sich von Cookies und Fingerprinting beim eigenen Chrome-Browser verabschiedet, hält Nauen Cookies nach wie vor für wichtig, um personenbezogene Werbung auszuspielen; andernfalls drohten eine Flut irrelevanter Werbung und vermehrt zahlungspflichtige Angebote. Wichtig sei außerdem, dass Anbieter von PIMS nicht zu „neuen Torwächtern“ würden.

Aus Sicht der Verbraucher kommt es darauf an, wie das TTDSG ausgelegt werde, so Verbraucherschützer Florian Glatzner vom Verbraucherzentrale Bundesverband. Er regte an, dass die Rechtsverordnung des Bundes möglichst viele Dienste einschließen möge, um den Verbraucherinnen und Verbrauchern individuelle Entscheidungen zu ermöglichen.

Ulrich Kelber sprach sich für datenminimierende Einwilligungsassistenten aus – sie könnten datensparsamer sein als eine zentrale Datenhaltung beim Einwilligungsmanagement, so der Bundesdatenschutzbeauftragte in einer Diskussionsrunde.

Die Konferenz endete mit einem Blick auf die Politik, der allerdings aufgrund der laufenden Koalitionsverhandlungen ohne konkrete Aussagen zur Politik der künftigen Bundesregierung auskommen musste. Grünen-Politiker und Innenexperte Konstantin von Notz und Ann Cathrin Riedel, Vorsitzende des LOAD e.V. und Vertreterin der Friedrich-Naumann-Stiftung waren sich einig, dass es gesamtgesellschaftliche Diskussionen und bürgerschaftliches Engagement brauche, um gute, gemeinwohlorientierte Datenpolitik umzusetzen.

Die Konferenz konnte im Live-Stream verfolgt werden; Mitschnitte der einzelnen Beiträge stehen auf der Website der Stiftung zum Nachschauen und -hören bereit.

ZU DEN AUFZEICHNUNGEN

→ https://sds-links.de/TTDSG

RÜCKBLICK: DATENTAG „DATENSCHUTZ IM DIGITALEN SCHULUNTERRICHT

WIE LÄSST SICH DIGITALER SCHULUNTERRICHT DATENSCHUTZGERECHT GESTALTEN?

Diese Frage stellten wir zum Beginn des neuen Schuljahres, also zu Beginn des mittlerweile vierten Halbjahrs unter Pandemie-Bedingungen. Ein Hauptstreitpunkt ist die Nutzung von Diensten, die internationale Datentransfers auslösen. Der Drittlandsbezug besteht dabei meist zu den USA. Dorthin fließen Daten, die aus Sicht der Datenschutzaufsicht nicht dorthin fließen dürfen, sei es aus den Videokonferenzen oder aus anderen digitalen Unterrichtswerkzeugen.

Wir sprachen dazu mit Beteiligten aller Interessengruppen: Mit Vertreterinnen von Kultusministerien ebenso wie mit Lehrkräften und Schülerinnen und Schülern; mit Bildungsexpert:innen, Anbietern von Videokonferenz-Software und natürlich mit der Datenschutzaufsicht, vertreten durch den Landesdatenschutzbeauftragten von Thüringen, der im Sommer vergangenen Jahres sogar Bußgelder gegen Lehrerinnen und Lehrer bei Nutzung der falschen Unterrichts-Tools in Aussicht gestellt hatte.

Direkt von Schülerinnen und Schülern wollten wir hören, welche Rolle der Datenschutz eigentlich im Unterricht und im Austausch mit der Schule spielt. Werden dort Datenschutz und Datensicherheit beim Umgang mit Schülerdaten angemessen thematisiert? Spielen die Rechte der Lernenden bei der Auswahl digitaler Instrumente eine Rolle? Die ernüchternde Antwort, kurz gefasst: Nein. Angesichts dessen, dass öffentlich stets betont wird, wie gefährdet die sensiblen Schülerdaten seien und welch hohe Aufmerksamkeit deren Schutz bedürfe, hat uns das erstaunt.

Wünschenswert erscheint uns, dass die Bildungsverantwortlichen in allen Bundesländern sich gegenüber datenschutzgerechten Lösungen offen zeigen. In einer zunehmend digitalisierten Lebenswelt muss der Kompetenz zum achtsamen Umgang mit Daten auch im Unterricht ein größerer Stellenwert eingeräumt werden.

Niemand weiß, ob wir in den kommenden Monaten wieder verstärkt zum Distanzunterricht in den Schulen zurückkehren müssen. Und niemand hofft, dass es so kommt. Aber natürlich müssen die Schulen vorbereitet sein. Doch Digitalisierung und Datenschutz müssen auch im Schulkontext zusammengedacht werden. Im Sinne des Schutzes der Rechte der Schülerinnen und Schüler sollte es heißen: Keine Digitalisierung von Bildungsmaßnahmen ohne Datenschutz. Daneben bleibt der Gesichtspunkt der Machbarkeit. Soweit datenschutzgerechte Werkzeuge noch nicht in der gesamten Schullandschaft verfügbar sind, brauchte es pragmatische Lösungen.

Wir haben die Konferenz aufgezeichnet und die Mitschnitte auf unserer Website veröffentlicht.

ZU DEN AUFZEICHNUNGEN

→ https://sds-links.de/schuldatenschutz

UNSERE GÄSTE WAREN

- **Christina Adamski**, Grundschullehrerin, Datenschutzbeauftragte beim Staatlichen Schulamt München
- **Ansgar Baums**, Zoom
- **Pascal Braun**, Berufsschüler Baden-Württemberg
- **Erich Clemens** / Friedrich-Magnus-Schwerd-Gymnasium, Speyer
- **Anna Dederichs**, Abiturientin, Rheinland-Pfalz
- **Yvonne Gebauer MdL**, Ministerin für Schule und Bildung des Landes Nordrhein-Westfalen
- **Dr. Marcus Hahn**, Deutscher Philologenverband
- **Dr. Lutz Hasse**, Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
- **Prof. Dr. Dieter Kugelmann**, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
- **Dr. Melanie Stilz**, Technische Universität Berlin / cyber4EDU e.V.
- **Benjamin Stingl**, Ministerium für Bildung des Landes Rheinland-Pfalz
- **Percy Ott**, Cisco
- **Lukas Wagner**, Schüler, Hessen
- **Daniel Zacharias**, Sdui

ÜBERBLICK: UNSERE VERÖFFENTLICHUNGEN

In den letzten Monaten sind haben wir unser Portfolio an regelmäßig erscheinenden Veröffentlichungen thematisch erweitert, daher hier ein aktueller Überblick:

Jeweils montags erscheint die **DatenschutzWoche** mit Datenschutzneuigkeiten aus der Welt und den Aufsichtsbehörden und den wichtigsten Gerichtsentscheidungen der Woche.

→ **Ältere Ausgaben und Anmeldung: https://sds-links.de/DatenschutzWoche**

Zwei- bis dreimal im Jahr erscheint der **Politikbrief**, der ein aktuelles Datenschutz-rechtliches oder -politisches Thema in den Blickpunkt stellt und ansonsten über unsere Arbeit berichtet

→ **Ältere Ausgaben: https://sds-links.de/politikbrief**

→ **Anmeldung: mail@stiftungdatenschutz.org**

An ehrenamtlich Engagierte richtet sich unsere Webinar-Reihe **"Datenschutz im Ehrenamt"**, Informationen, Aufzeichnungen der Webinare und Anmeldung zum Newsletter:

→ **https://sds-links.de/ehrenamt**

Und schließlich betreiben wir das **Zentralarchiv** für die Tätigkeitsberichte der Datenschutzaufsichtsbehörden des Bundes und der Ländern, sowie ausgewählter **kirchlicher Einrichtungen** und öffentlich **rechtliche Sendeanstalten**.

→ **https://zaftda.de**

→ **Anmeldung: zaftda-news@stiftungdatenschutz.org**

AUSBLICK

Nachdem der DatenTag „Das TTDSG und neue Wege zur Einwilligungsverwaltung“ am 3. November vor Publikum stattfinden konnte, kehren wir für die nächste Konferenz pandemiebedingt zurück zu einem Online-Format. Am 13. Dezember diskutieren wir auf unserem **DatenTag „Datenschutz und Künstliche Intelligenz“** mit hochrangigen Expertinnen und Experten, wie sich Künstliche Intelligenz verantwortungsvoll und vor allem datenschutzgerecht einsetzen lässt. Wir erläutern die Chancen und Risiken von Künstlicher Intelligenz für das Datenschutzrecht und das Antidiskriminierungsrecht und stellen Initiativen aus Forschung und Praxis vor.

PROGRAMM UND ANMELDUNG
→ https://sds-links.de/DSundKI

Datenschutz spielt auch im Ehrenamt eine wichtige Rolle. Ehrenamtlich Engagierte, Vereine, gemeinnützige Organisationen suchen pragmatische Hilfe bei der Umsetzung datenschutzrechtlicher Vorgaben. Sie möchten wir mit unseren Informationsangeboten praxisorientiert unterstützen. Im Dezember veröffentlichen wir daher die **Handreichung "Datenschutz im Verein"**, die vor allem kleinen Vereinen die grundlegenden datenschutzrechtlichen Vorgaben praxisnah, in verständlicher Sprache und ohne komplizierte juristische Details zugänglich machen soll.

In Vorbereitung ist derzeit auch eine umfangreiche **Arbeitshilfe "Datenschutz für das Ehrenamt"**. Darin werden vereinstypische Themen wie die Mitgliederverwaltung, Kommunikation im Verein, Webseite, Fotos und viele andere detailliert in Hinblick auf die datenschutzrechtlichen Aspekte erläutert. Danebengibt es konkrete praktische Tipps, Mustervorlagen, Links und Checklisten. Die Arbeitshilfe ist modular aufgebaut und wird kontinuierlich gepflegt und ergänzt.

IHRE ANSPRECHPARTNER

FREDERICK RICHTER, LL.M.
Vorstand
richter@stiftungdatenschutz.org

PROF. DR. ANNE RIECHERT
Wissenschaftliche Leiterin
a.riechert@stiftungdatenschutz.org

WIEBKE FRÖHLICH
Wissenschaftliche Mitarbeiterin
wiebke.froehlich@stiftungdatenschutz.org

HENDRIK VOM LEHN
Berater für Datenschutz und Informationssicherheit
h.vomlehn@stiftungdatenschutz.org

CRISTINA BITTNER
Beraterin für Datenschutz und Informationssicherheit
c.bittner@stiftungdatenschutz.org

ANTJE SIMON (M.A.)
Büroleitung
a.simon@stiftungdatenschutz.org

UNSER ARCHIV ALLER POLITIKBRIEFE FINDEN SIE HIER

politikbrief.stiftungdatenschutz.org

IMPRESSUM

Herausgeber

Stiftung Datenschutz

Karl-Rothe-Straße 10 –14
04105 Leipzig
T 0341 5861 555-0
F 0341 5861 555-9
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

Redaktionsleitung und Mitarbeit

Anne Riechert, Antje Simon, Florian König

Redaktionsschluss
22. November 2021

Agenturpartner

KING CONSULT | Kommunikation