**Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen**

LDI NRW, Postfach 20 04 44, 40102 Düsseldorf

Bundesministerium für Wirtschaft und Energie

info@bmwi.bund.de

rolf.bender@bmwi.bund.de

Nachrichtlich:

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie
des Landes Nordrhein-Westfalen

poststelle@mwide.nrw.de

Aktenzeichen
bei Antwort bitte angeben
41.2.1-18

Frau Robke
Telefon 0211 38424--41
Fax 0211 38424-10

Referentenentwurf für ein TTDSG
Ihr Schreiben vom 12.01.2021; Az.: VIB2-63204/012#001

Sehr geehrte Damen und Herren,

ich danke Ihnen für die Möglichkeit, Stellung zu dem neuen Referentenentwurf des TTDSG nehmen zu können.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) macht gerne davon Gebrauch, ebenso zu den unter Ziffer 1. bis 4. Ihres Anschreibens aufgeworfenen Fragen Stellung zu nehmen.

Lassen Sie mich zunächst betonen, dass wir ein Inkrafttreten des TTDSG grundsätzlich befürworten würden, da es in vielen Bereichen für mehr Klarheit sorgen und längst überfällige Umsetzungen von EU-Richtlinien vollziehen würde.

Insbesondere die neue Cookie-Regelung in § 22 ist in diesem Zusammenhang zu erwähnen. In der Vergangenheit gab es häufig Unsicherheiten dahingehend, welches Gesetz auf das Setzen und Auslesen von Cookies und anzuwenden ist. Während die Datenschutzaufsichtsbehörden in ihrer Orientierungshilfe Telemedien für nicht-öffentliche Stellen

Dienstgebäude und Lieferanschrift:
Kavalleriestraße 2 - 4
40213 Düsseldorf
Telefon 0211 38424-0
Telefax 0211 38424-10
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 708, 709
Haltestelle Poststraße

von März 2019 (abrufbar unter https://www.datenschutzkonferenz-online.de/orientierungshilfen.html) betonen, dass die Datenschutzregeln des TMG (§§ 11 ff.) nach Wirksamwerden der DS-GVO nicht mehr anwendbar sind, da insbesondere die Cookie-Regeln der EU-ePrivacy-Richtlinie niemals richtig umgesetzt wurden, geht der BGH in seinem Urteil vom 28. Mai 2020 (Az. I ZR 7/16; „Planet49-Urteil") davon aus, dass man das Einwilligungserfordernis in die entsprechende Regel des § 15 Abs. 3 TMG entgegen seinem Wortlaut hineinlesen muss. In dem Entwurf zum TTDSG wird nunmehr die Auffassung der Datenschutzaufsichtsbehörden dahingehend bestätigt, dass die Datenschutzregeln des TMG wegen der DS-GVO nicht mehr anwendbar sind. Mit dem § 22 ist nunmehr eine Regelung vorgesehen, die die Vorgaben der EU-ePrivacy-Richtlinie adäquat umsetzt und sich eng an den Wortlaut des Art. 5 Abs. 3 ePrivacy-Richtlinie orientiert. Dies wird ausdrücklich begrüßt.

Die aufgrund des in § 22 verwendeten Begriffs der „Endeinrichtung" anstatt „Endgerät" stattfindende Erweiterung des Anwendungsbereichs auch auf im „Internet der Dinge" an das öffentliche Kommunikationsnetz angeschlossene Gegenstände, wie etwa Smarthome-Anwendungen, befürworten wir ebenfalls.

Zu den von Ihnen aufgeworfenen vier Regelungsfragen nehmen wir wie folgt Stellung:

Zu 1.) Zur Frage der Erforderlichkeit von Regelungen zu Datenmanagementsystemen und Personal Information Management-Services (PIMS):

Da die geplante Verordnung Data Governance Act voraussichtlich Regelungen dazu enthält, ist nachvollziehbar, dass hier derzeit keine Regelungen getroffen werden.

Zu 2.) Zur Frage, ob eine Regelung zu Browsereinstellungen im TTDSG für sinnvoll erachtet wird, die verhindern soll, dass Browser herstellerseitig so eingestellt werden, dass der Zugriff auf die Informationen in Endeinrichtungen verhindert wird, auch wenn der Nutzer eingewilligt hat:

Sofern die geplante Regelung darauf abzielen soll, grundsätzlich datenschutzfreundliche Voreinstellungen von Browsern zu verhindern, sprechen wir uns dagegen aus. Aus Erwägungsgrund 78 Satz 3 DS-GVO ergibt sich aus unserer Sicht eine Aufforderung der Hersteller, datenschutzfreundliche Voreinstellungen in ihre Endgeräte zu implementieren. Hier heißt es: „*In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von*

personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen."

Auch die EU-Kommission fordert Unternehmen und Organisationen ausdrücklich auf, technische und organisatorische Maßnahmen in den frühesten Stadien der Gestaltung der Verarbeitungsvorgänge so zu implementieren, dass die Grundsätze des Schutzes der Privatsphäre und des Datenschutzes von Anfang an gewährleistet sind ("Datenschutz durch Technik"). Standardmäßig sollten Unternehmen/Organisationen nach Auffassung der Kommission sicherstellen, dass personenbezogene Daten mit dem höchsten Datenschutzniveau verarbeitet werden (das Statement der EU-Kommission ist abrufbar unter https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en).

Sollte es bei der geplanten Regelung lediglich darum gehen, sicherzustellen, dass (datenschutzfreundliche) Browsereinstellungen nicht dazu führen, dass Einwilligungen der Nutzer in konkrete Verarbeitungen ihrer personenbezogenen Daten nicht berücksichtigt werden, sollte die Regelung so ausgestaltet werden, dass die Gerätehersteller aufgefordert werden, Endgeräte datenschutzfreundlich zu konfigurieren.

Zu 3.) Zur Frage, ob die Aufnahme einer Regelung zum Ausschluss der Rufnummernunterdrückung für im Einzelfall festgelegte zentrale Rufnummern von Strafverfolgungsbehörden für sinnvoll gehalten wird:

Es soll eine Beschränkung auf im Einzelfall festgelegte zentrale Nummern von Strafverfolgungsbehörden erfolgen. Dies klingt nach einer begrenzten Zahl. Uns stellt sich daher – insbesondere auch vor dem Hintergrund der bereits bestehenden Regelungen des § 102 Abs. 8 und § 108 Abs. 1 S. 3 Nr. 2 TKG – die Frage, ob das Vorhaben wirklich zielführend ist.

Zudem möchten wir folgende Fragen aufwerfen: Gibt es statistische Daten darüber, in wie vielen Fällen sich aus Anrufen bei Nummern, die von einer solchen neuen Regelung betroffen sein

könnten, ein Anfangsverdacht für eine Straftat bzw. konkrete Hinweise für eine Gefahrenabwehr ergeben haben und es für die Strafverfolgung bzw. Gefahrenabwehr hinderlich war, dass die Rufnummernunterdrückung aktiv war? In wie vielen Fällen davon hat sich im Nachhinein der Verdacht einer Straftat bzw. Gefahr bewahrheitet, so dass es auch aus ex post-Sicht hilfreich gewesen wäre, wenn die anrufende Person hätte ermittelt werden können? In welchem Verhältnis stehen diese Zahlen zur Gesamtzahl der Notrufe?

Wir weisen darauf hin, dass die geplante Regelung hauptsächlich dazu führen würde, dass Daten von Personen erfasst werden, die keinen Anlass für eine Datenerfassung gegeben haben.
Darüber hinaus sehen wir das Problem, dass das Vorhaben ggf. die Akzeptanz der Notfallnummer senkt. Betroffene könnten Nachteile eines Anrufs befürchten und von der Meldung einer Gefahr oder Straftat Abstand nehmen. Gibt es hierzu Erfahrungen mit den o. g. Regelungen bezüglich der Rufnummern 112 und 110?

Ferner besteht aus unserer Sicht das Risiko, dass die Anrufdaten nicht nur in Anschlagsfällen verwendet werden. Beispielsweise würden so auch Rückfragen bei Personen möglich, die selbst weder potentielle Gefährder noch Verdächtige einer Straftat sind und aus persönlichen Motiven anonym bleiben wollten.

Im Ergebnis ist daher zu befürchten, dass die Nachteile die zu erwartenden Vorteile einer solchen Regelung überwiegen.

Zu 4.) Zur Frage, ob die vom BMWi befürwortete Aufnahme einer gesetzlichen Verpflichtung von Anbietern von Telemedien zur Erhebung und Verifizierung von Name, Adresse und Geburtsdatum der Nutzer, erfolgen sollte:

Aus unserer Sicht ist es völlig unverhältnismäßig, jeden Nutzer, der sich im Internet bewegt, identifizierbar zu machen.
Staatliche Stellen erhalten in zunehmenden Maße Möglichkeiten, entsprechendes Handeln personenscharf nachzuvollziehen. Solche Maßnahmen sollten nur zugelassen werden, wenn sie wirklich erforderlich sind. Insbesondere sollte zunächst eine Evaluation des Ist-Zustandes und der zu erwartenden Verbesserungen erfolgen. Der zu erwartende Nutzen muss dann mit den mit der Maßnahme verbundenen Nachteilen für rechtschaffene Bürgerinnen und Bürger abgewogen werden.
Vor diesem Hintergrund stellt sich uns in diesem Zusammenhang die Frage, ob zuvor eine Evaluation durchgeführt wurde, in wie

vielen Fällen das Vorhandensein dieser Möglichkeiten einen messbaren Vorteil gegenüber der jetzigen Rechtslage gehabt hätte. Diese Fälle müssten ins Verhältnis zu allen Nutzungen von Telemedien etc. gesetzt werden. Auch sollte in diesem Kontext analysiert werden, welchen Nutzen beispielsweise die vergleichbare Regelung zu Handy-Prepaid-Verträgen bislang gehabt hat. Wurde diese Maßnahme evaluiert?

Die generelle Identifizierbarkeit von Nutzern im Internet würde bewirken, dass Telemedien grundsätzlich nicht mehr anonym genutzt werden könnten. Nutzer müssten für jede aufgerufene Website ihre personenbezogenen Daten hinterlassen. Dies stellt nicht zuletzt auch einen Verstoß gegen den in Art. 5 Abs. 1 c DS-GVO normierten Grundsatz der Datenminimierung dar.

Hinzu kommt, dass ein Telekommunikationsdienste-Anbieter, für den solche Verpflichtungen schon nach derzeitiger Rechtslage teilweise gelten, einem gänzlich anderen Aufsichtsregime unterliegt. Das TKG sieht z. B. eine Meldepflicht für TK-Anbieter vor (§ 6 TKG). Hinzu kommen zahlreiche Prüfungs- und andere Pflichten, deren Einhaltung die Bundesnetzagentur überwacht. Solche Regelungen gelten für Telemedienanbieter nicht. Im Prinzip kann jedermann jederzeit eine Website veröffentlichen, wobei er „lediglich" die Impressums- und Datenschutzregeln einhalten muss. Auch vor diesem Hintergrund ist die Verpflichtung zur Nutzeridentifikation zu hinterfragen, denn sie birgt nicht unerhebliche Risiken für die personenbezogenen Daten der Nutzer. Bereits nach geltender Rechtslage müssen wir feststellen, dass sich zahlreiche Websitebetreiber häufig nicht an die Vorgaben der Datenschutzregeln halten und z. B. personenbezogene Nutzerdaten an Dritte ohne entsprechende Rechtsgrundlage weitergeben.

Im Übrigen merken wir an, dass das TKG für die Nutzung von E-Mail-Diensten (auf die vor dem GMail-Urteil des EuGH v. 13. Juni 2019, C-193/18, das TKG angewendet wurde) bislang nicht verbindlich vorgeschrieben hat, dass Nutzer sich identifizieren. § 111 Abs. 2 TKG sieht vor, dass der Provider Daten des Nutzers erheben *kann*, es gilt aber keine Verpflichtung, das auch zu tun. Auch dies kann daher nicht Argument für die Einführung der vom BMI vorgeschlagenen Regelung dienen.

Aus unserer Sicht sollte daher auf die Aufnahme einer solchen Regelung verzichtet werden und die Vorschrift des § 13 Abs. 6 TMG erhalten bleiben.

Mit freundlichen Grüßen
im Auftrag
S. Robke
(Robke)