1 von 4

Vereinfachte wirkungsorientierte Folgenabschätzung

Einbringende Stelle:	BKA
Vorhabensart:	Bundesgesetz
Laufendes Finanzjahr:	2019
Inkrafttreten/ Wirksamwerden:	2020

Vorblatt

Problemanalyse

In online-Foren veröffentlichen Nutzer immer mehr rechtswidrige Postings wie insbesondere sogenannte Hass-Postings, die oft auch strafrechtlich relevant sind oder auf andere Weise den Persönlichkeitsschutz beeinträchtigen. In vielen Fällen verwenden Poster dabei "Nicknames" (Phantasienamen) oder vermeintliche Klarnamen (bspw. Max Mustermann, Alex Ander), ohne dass die Diensteanbieter, die ein Forum betreiben, diesen eine reale Person zuordnen zu können. Dieser Tatsache begünstigt derartige den Persönlichkeitsschutz verletzende Inhalte. Dazu kommen rechtliche und technische Schwierigkeiten bei der Identifizierung von Nutzern, die solche rechtswidrigen Postings veröffentlicht haben. Bei der im Entwurf vorgesehenen Lösung konnte auch darauf Bedacht genommen werden, dass es bereits verschiedene Beispiele von verschiedenen Anbietern von Foren gibt, bei denen sich der User „verifizieren“ lassen kann, etwa indem er einen geeigneten Identitätsnachweis vorlegt.

Ziel(e)

Erleichterung der Verfolgung von Rechtsansprüchen im Falle rechtswidriger Postings

Förderung des respektvollen Umgangs der Poster in online-Foren miteinander

Inhalt

Das Vorhaben umfasst folgende Maßnahme(n):

Verpflichtung der Diensteanbieter, die Foren betreiben oder die Einrichtung eines Forums ermöglichen, die Identität der Poster zu überprüfen; die Wahl der Mittel, wie dies bewerkstelligt wird, bleibt den Diensteanbietern überlassen; erst nach erfolgreichem Abschluss des Registrierungsprofils soll der Nutzer Postings in diesem Forum veröffentlichen können.

Nutzer haben ein Registrierungsprofil zu erstellen, und sich unter Angabe jedenfalls von Vorname, Familienname zu registrieren; die Verpflichtung, nach denen die personenbezogenen Daten Gerichten, Verwaltungsbehörden zu übermitteln sind, bestimmt sich nach den Regelungen des § 4 des Entwurfs

Verpflichtung der Diensteanbieter zur Bestellung eines verantwortlichen Beauftragten, insbesondere als Zustellbevollmächtigten.

KommAustria als Aufsichtsbehörde kann Sanktionen über Diensteanbieter verhängen.

Beitrag zu Wirkungsziel oder Maßnahme im Bundesvoranschlag

Das Vorhaben hat keinen direkten Bezug zu einem Wirkungsziel.

Finanzielle Auswirkungen auf den Bundeshaushalt und andere öffentliche Haushalte

Aus der gegenständlichen Maßnahme ergeben sich mit Ausnahme der aus dem Bundeszuschuss nach § 35 KOG zu bestreitenden Kosten für die Aufsicht keine finanziellen Auswirkungen für den Bund, die Länder, die Gemeinden oder für die Sozialversicherungsträger.

Anmerkungen zu sonstigen Auswirkungen (in Wirkungsdimensionen gemäß § 6 Abs. 1 WFA-GV):

Finanzielle Auswirkungen auf den Bundeshaushalt und andere öffentliche Haushalte: Es ist davon auszugehen, dass die KommAustria die ihr mit diesem Gesetzesentwurf übertragenen Aufgaben innerhalb

der vorhandenen Ressourcen abzudecken in der Lage ist. Es ergeben sich keine finanziellen Auswirkungen für die Länder oder Gemeinden oder auf die Sozialversicherungsträger.

Auswirkungen auf die Verwaltungskosten für Unternehmen: Auf der Grundlage der in § 3 Abs. 2 des Entwurfs vorgesehenen Eingrenzung des Anwendungsbereichs auf bestimmte Diensteanbieter mit mehr als 100.000 registrierten Nutzern oder einem jährlichen Umsatz von über 500.000 Euro sowie auf die mit Förderungsnehmern nach dem PresseFG im Verbund stehenden sogenannte „publisher“, die Online-Informationsangebote mit Foren bereitstellen, werden etwa 50 Unternehmen von den Verpflichtungen betroffen sein, die nach derzeitigem Wissensstand in einer Betrachtung über 4 Jahre weniger als 100.000 Euro pro Jahr ausmachen werden.

Auch sonst zeigt das Vorhaben keine wesentlichen Auswirkungen in den Wirkungsdimensionen gemäß § 6 Abs. 1 WFA-GV (Wesentlichkeitsgrenzen wie in Anlage 1 WFA-GV) und löst auch keine finanziellen Auswirkungen aus, die die relevanten Betragsgrenzen für eine vereinfachte WFA übersteigen. Das Vorhaben hat ferner keine langfristigen finanziellen Auswirkungen gemäß § 9 WFA-FinAV und steht in keinem direkten substanziellen inhaltlichen Zusammenhang mit Angaben zur Wirkungsorientierung im BFG.

Verhältnis zu den Rechtsvorschriften der Europäischen Union

Die vorgesehenen Regelungen beziehen sich auf Dienste der Informationsgesellschaft im Sinne von § 1 Abs. 1 Z 2 des Bundesgesetzes zur Durchführung eines Informationsverfahrens auf dem Gebiet der technischen Vorschriften, der Vorschriften für die Dienste der Informationsgesellschaft und der Normen (Notifikationsgesetz 1999 – NotifG 1999), BGBl. Nr. 183/1999, und sind daher der Kommission vor ihrer Erlassung zu notifizieren.

Innerhalb einer Stillhaltefrist von drei Monaten darf der Entwurf nicht erlassen werden; diese Frist kann sich unter bestimmten Voraussetzungen auch verlängern (vgl. § 3 NotifG 1999). Die Stillhaltefrist dient dazu, dass die Kommission und die anderen Mitgliedstaaten den Entwurf prüfen und dazu Stellungnahmen abgeben können (insbesondere über mögliche Beeinträchtigungen des freien Warenverkehrs, des freien Verkehrs von Dienstleistungen oder der Niederlassungsfreiheit im Rahmen des Binnenmarktes), die bei der weiteren Ausarbeitung der Vorschriften so weit wie möglich zu berücksichtigen sind (vgl. Art. 5 und 6 der Richtlinie (EU) 2015/1535 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. L 241 vom 17. September 2015, S. 1).

Weiters knüpfen einzelne der vorgesehenen Regelungen an das Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz – ECG), BGBl. I Nr. 152/2001, zuletzt geändert durch das BGBl. I Nr. 34/2015, als Umsetzungsmaßnahme zur Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. L 178 vom 17. Juli 2000, S. 1, und an die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4. Mai 2016, S. 1, an.

Die E-Commerce Richtlinie räumt – was sich aus Art 3 Abs. 4 lit a 1. Fall ergibt – unter bestimmten Voraussetzungen den Mitgliedstaaten die Möglichkeit ein, Maßnahmen auch gegenüben ausländischen Anbietern zu ergreifen, wenn dies zum Schutz der öffentlichen Ordnung, insbesondere Verhütung, Ermittlung, Aufklärung und Verfolgung von Straftaten, einschließlich der Bekämpfung der Hetze aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität, sowie von Verletzungen der Menschenwürde einzelner Personen notwendig ist und die Maßnahmen in einem angemessenen Verhältnis zu diesen Schutzzielen stehen.

Besonderheiten des Normerzeugungsverfahrens

Keine.

Datenschutz-Folgenabschätzung gem. Art 35 EU-Datenschutz-Grundverordnung

Im Rahmen einer nach Art. 35 Abs. 10 DSGVO vorgesehenen Folgenabschätzung ist zu prüfen, ob die Datenverarbeitung „*voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen*“ iSd Art. 35 Abs. 1 zur Folge hat.

Art. 35 Abs. 7 DSGVO legt für die Vornahme dieser Folgenabschätzung folgende Inhalte fest:

a) Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Eine Prüfung ergibt, dass die Voraussetzungen des Art. 35 Abs. 10 DSGVO vorliegen. Zu den Voraussetzungen des vorzitierten Abs. 7 ist im Einzelnen Folgendes auszuführen:

Im Sinne einer systematischen Beschreibung der geplanten Verarbeitungsvorgänge, der Zwecke sowie der berechtigten Interessen ist auszuführen, dass Vorname, Nachname und Adresse natürlicher Personen von den Dienstanbietern erfasst werden sollen, um sie als „Zutrittsbedingung“ zur Teilnahme an der Kommunikation in einem bereitgestellten Forum auf ihre Richtigkeit zu prüfen. Diese Daten werden ausschließlich gegenüber dem Diensteanbieter bekanntgegeben; die Verwendung von „Nicknames“ im Forum wird weiterhin uneingeschränkt zulässig bleiben. Ausschließlich in den nach § 4 des Entwurfs beschriebenen Fällen ist (ident wie derzeit schon nach dem TKG und der stopp) eine Übermittlung an Gerichte, Behörden und zusätzlich (neu) an dritte Personen unter detailliert beschriebenen zwingenden Voraussetzungen vorgesehen. Das angestrebte Ziel der Ermöglichung der Rechtsverfolgung für Dritte in den Fällen der Privatanklagedelikte und der Geltendmachung von Ansprüchen nach § 1330 ABGB kann nicht – als gelinderes Mittel – allein über den Weg der IP-Adresse erreicht werden: Entgegen der Ansicht, dass eine eindeutige Zuordenbarkeit eines Kommunikationsvorgangs zu einem Teilnehmer, dem eine IP-Adresse zu einem bestimmten Zeitpunkt unter der Angabe der zugrundeliegenden Zeitzone zugeteilt war, möglich wäre, kann nach einhelliger Meinung von Experten das aufklärungstechnische Ziel, eine Identifizierung von Nutzern im Falle von Netzwerkadressübersetzung NAT (Network Address Translation, NAT) innerhalb von lokalen Netzwerken zu erreichen, in den allermeisten Fällen aus technischen Gründen nicht erreicht werden, und zwar unabhängig vom betriebenen Aufwand (so müsste jeder Betreiber pro Sekunde etwa 200.000 Datensätze speichern), weil die für eine Zuordnung von internen Adressen in lokalen Netzwerken die darüber hinaus erforderlichen Port-Nummern üblicherweise nur ganz selten bekannt sind. (Vgl. die RV zum Bundesgesetz, mit dem das Telekommunikationsgesetz 2003, das Funkanlagen-Marktüberwachungs-Gesetz, das Funker-Zeugnisgesetz 1998, das Postmarktgesetz, das Gebäude- und Wohnungsregister-Gesetz und das KommAustria-Gesetz geändert werden, Rz 87 (§ 92 Abs. 3 Z 16a) und Rz 105 (§ 99 Abs. 2 neuer zweiter Satz), RV 257 BlgNR XXVI. GP, sowie den sich darauf beziehenden Bericht des Verkehrsausschusses über diese RV (257 d.Blg.), 315 BlgNR StenProt XXVI. GP, S. 2, zur Begründung des beantragten Entfalls der beiden genannten Änderungen (Rz 87 und 105)).

Zur Bewertung der Notwendigkeit und Verhältnismäßigkeit kann angemerkt werden, dass die im SVN-G enthaltenen Regelungen über die Ermittlung und Speicherung von Daten einem von Art. 10 Abs. 2 EMRK anerkannten Ziel, nämlich dem Schutz der Rechte Dritter durch die Verbesserung der Verfügbarkeit der Daten im Falle von Verletzungen von Bestimmungen zum Persönlichkeitsschutz dienen. Die Notwendigkeit ergibt sich aus dem wichtigen öffentlichen Interesse an einer Rechtsverfolgung, die ohne die Verfügbarkeit der betreffenden Daten scheitert. Gesondert ist darauf hinzuweisen, dass – wie § 4 Abs. 4 des Entwurfs dies eindeutig regelt – beim Diensteanbieter keine Verknüpfung zwischen der Identität eines Posters und dem Inhalt eines Postings vorgenommen werden darf.

Es bestehen keinerlei Anhaltspunkte, dass ein gesteigertes Risiko für in Erwägungsgrund 85 der Datenschutz-Grundverordnung unter anderem genannte *„physische, materielle oder immaterielle Schäden“, „Verlust der Kontrolle über personenbezogene Daten“* bestünde. Die Anforderung der Authentifizierung soll im Gegenteil die weiters genannten Problembereiche *„Identitätsdiebstahl oder -betrug“* oder auch *„Rufschädigung“* mit angemessenen Mitteln beseitigen. Wer Daten zur Rufschädigung missbraucht, geht angesichts der gerichtlichen Strafdrohung in §§ 111 StGB selbst ein hohes Risiko ein.

Ein Risiko der *„Diskriminierung“* ist ebensowenig zu erkennen und es kommt auch zu keiner „*Einschränkung der Rechte der betroffenen Personen*“. „*Finanzielle Verluste*“ (wie ebenfalls in ErwG 85 angesprochen) sind nicht zu erwarten, da keine Finanzdaten verwendet werden.

Ein „*Verlust der Vertraulichkeit bei Berufsgeheimnissen*“ ist ausgeschlossen, weil derartige Fakten nicht erhoben werden. Es ist schließlich auch nicht zu erkennen, wodurch sonst „*erhebliche wirtschaftliche oder gesellschaftliche Nachteile*“ eintreten könnten.

Diese Risiken sind nach Erwägungsgrund 75 der DSGVO mit Eintrittswahrscheinlichkeit und Schwere anzugeben. Hierzu ist zu bemerken, dass sich die Zahl der Anzeigen wegen Hackings (§ 118a StGB) im Jahr 2017 um 20,6 Prozent verringert hat und auf 363 gesunken ist (vgl. https://bundeskriminalamt.at/501/files/PKS_17_Broschuere_Web.pdf, Seite 17 [zuletzt abgerufen 11.4.2019]. Angesichts bloß vereinzelter Verurteilungen nach § 118a StGB oder auch nach § 126a im Jahr 2017 (vgl. Statistik Austria, Gerichtliche Kriminalstatistik 2017, http://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/soziales/kriminalitaet/index.html [11.4.2019]) sowie einer Zahl von ca 3,7 Mio. aktiven IT-Systemen in Österreich ergibt sich eine äußerst geringe Wahrscheinlichkeit, dass sich die von der Datenschutz-Grundverordnung angeführten Risiken verwirklichen. Die Zahl von 3,7 Mio. aktiven IT-Systemen ergibt sich aus der Zahl der Privathaushalte, die für das Jahr 2017 mit 3 890 000 beziffert wird (Statistik Austria, Haushaltsstatistik 2017, https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/bevoelkerung/haushalte_familien_lebensformen/haushalte/index.html [19.2.209]), der Zahl der Unternehmen, die für das zuletzt erfasste Jahr 2016 mit 330 000 beziffert wird (Statistik Austria, Unternehmens, Arbeitsstättenstatistik 2016, https://www.statistik.at/web_de/statistiken/wirtschaft/unternehmen_arbeitsstaetten/index.html [11.4.2019]) sowie dem Faktor der IKT-Nutzung der für das Jahr 2018 für private Nutzerinnen und Nutzer mit rund 87 Prozent und für Unternehmen mit 99 Prozent (https://www.statistik.at/web_de/statistiken/energie_umwelt_innovation_mobilitaet/informationsgesellschaft/ikt-einsatz_in_unternehmen/index.html [19.2.2019]).

Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in Erwägungsgrund 78 der DSGVO unter anderem auch die „*Minimierung der Verwendung/Verarbeitung personenbezogener Daten*“ genannt. In diesem Sinn beschränkt sich die gesetzliche Regelung auf das Minimum der zur Durchführung einer Authentisierung und für eine Rechtsverfolgung im Falle der Privatanklage und von Ansprüchen nach § 1330 ABGB erforderlichen Angaben. Die ausdrückliche und abschließende Regelung des § 4 SVN-G macht deutlich, dass eine Weitergabe zu anderen Zwecken verboten ist; entsprechend Art. 17 der DSGVO ist das Recht des Nutzers vorgesehen, zu verlangen, dass sein Registrierungsprofil unverzüglich gelöscht wird. Hinzu tritt die zeitliche Beschränkung der Speicherdauer insbesondere auch bei routinemäßig vorgenommenen Überprüfungsvorgängen bei festgestellter längerer Inaktivität.

Diese Folgenabschätzung wurde mit der Version 5.5 des WFA – Tools erstellt (Hash-ID: 1129593559).