REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.210/0002-DSR/2015
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Justiz

Per Mail:
christian.pilnacek@bmj.gv.at
team.s@bmj.gv.at

Betrifft: **Bundesgesetz, mit dem das Strafgesetzbuch, das Suchtmittelgesetz, die Strafprozessordnung 1975, das Aktiengesetz, das Gesetz vom 6. März 1906 über Gesellschaften mit beschränkter Haftung, das Gesetz über das Statut der Europäischen Gesellschaft, das Genossenschaftsgesetz, das ORF- Gesetz, das Privatstiftungsgesetz, das Versicherungsaufsichtsgesetz 2016, und das Spaltungsgesetz geändert werden**
(Strafrechtsänderungsgesetz 2015)
Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **224. Sitzung am 24. April 2015 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Mit dem Entwurf sollen die seit dem Inkrafttreten des StGB 1975 eingetretenen **Veränderungen der gesellschaftlichen Rahmenbedingungen**, insbesondere der Werthaltungen, aber auch des technischen Fortschrittes im gerichtlichen Strafrecht so abgebildet werden, dass es auf gesellschaftliche Akzeptanz und Verständnis stößt und auf diese Weise in vollem Umfang die erforderliche Präventionswirkung entfalten kann. Seit Inkrafttreten des StGB 1975 hat sich auch das Verständnis von den Strafzwecken verändert, einzelne Entwicklungen, wie z.B. die neuen Tatbestände der

beharrlichen Verfolgung und der fortgesetzten Gewaltausübung machen die Orientierung anhand opferbezogener Faktoren deutlich.

Das **Vorhaben „StGB 2015“** fand Eingang in das **Arbeitsprogramm der österreichischen Bundesregierung 2013 – 2018** und wurde unter Bundesminister Univ. Prof. Dr. Wolfgang Brandstetter fortgesetzt.

Nach der konstituierenden Eröffnungssitzung der **Arbeitsgruppe** am 27. Februar 2013 traf sich diese zu insgesamt 14 weiteren Sitzungen. Resultierend aus den erzielten Ergebnissen und Vorschlägen wurde ein **Bericht** (Bericht der Arbeitsgruppe „StGB 2015“) verfasst, der Ende September dem Parlament übermittelt wurde (Bericht III 104 d.B. XXV. GP) und Gegenstand der Diskussion in der 4. Sitzung des Justizausschusses am 14. Oktober 2014 war.

Die im Bericht enthaltenen **Empfehlungen der Arbeitsgruppe „StGB 2015“** bilden die **Grundlage** für den vorliegenden Entwurf. Sie beinhalten zahlreiche Vorschläge zur Strafenrelation im Sinne einer Senkung der Strafdrohungen im Bereich der Vermögensdelikte und einer Anhebung der Strafdrohungen für die qualifizierte Körperverletzung. Weiters wird eine Neugestaltung der Fahrlässigkeitsdelikte, insbesondere die Schaffung eines eigenen Tatbestandes „grob fahrlässige Tötung“ empfohlen. Dem technischen Fortschritt wird vor allem durch die Empfehlungen im **Cybercrime-Bereich** und dem Vorschlag eines neuen Tatbestandes des **Ausspähens von Daten eines unbaren Zahlungsmittels** Rechnung getragen. Den **sozialen Medien** kommt in der heutigen Zeit eine große Bedeutung zu, weshalb die Arbeitsgruppe es für erforderlich hielt, dem unerwünschten neuen gesellschaftlichen Phänomen „**Cybermobbing**“ mit einer eigenen Strafbestimmung im StGB entgegenzuwirken. Schließlich wird auch eine Vereinheitlichung und Vereinfachung hinsichtlich der Strafdrohungen von Bestimmungen, welche eine Geldstrafe alternativ zu einer Freiheitsstrafe vorsehen, angesprochen, die mit der vorgeschlagenen Aufnahme einer alternativ angedrohten Geldstrafe in allen Delikten mit einer Strafdrohung bis zu einem Jahr Freiheitsstrafe erreicht werden soll.

2.) Datenschutzrechtliche relevante Bestimmungen

Mit diesem Entwurf zum Strafrechtsänderungsgesetz 2015 soll auch die Richtlinie 2013/40/EU des Europäischen Parlament und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates umgesetzt werden. Die innerstaatliche Umsetzung dieser

Richtlinie hat bis 4. September 2015 zu erfolgen. Diese Richtlinie umfasst im wesentlichen Straftatbestände, die bereits von den Bestimmungen des Computerstrafrechts umfasst sind. Allerdings sieht die gegenständliche Richtlinie in Artikel 9 vor, dass Mitgliedstaaten die erforderlichen Maßnahmen treffen, um sicherzustellen, dass die Straftaten mit wirksamen, angemessenen und abschreckenden Strafen, also mit entsprechend – differenzierten – Strafen geahndet werden. Wobei Abs. 5 bestimmt, dass die Mitgliedstaaten die erforderlichen Maßnahmen treffen, um sicherzustellen, dass der Missbrauch der personenbezogenen Daten einer anderen Person mit dem Ziel, das Vertrauen eines Dritten zu gewinnen, wodurch dem rechtmäßigen Identitätseigentümer ein Schaden zugefügt wird, im Einklang mit dem nationalen Recht **als erschwerender Umstand bei der Begehung von Straftaten** eingestuft werden kann, soweit der betreffende Umstand nicht bereits eine andere Straftat im Sinne des nationalen Rechts darstellt. Nachdem in diesem Absatz 5 der digitale Missbrauch von (Identitäts)Daten (sog. „Identitätsdiebstahl“) angesprochen wird, stellt sich für den Datenschutzrat die Frage, warum das BMJ von dieser Möglichkeit abgesehen hat und kein diesbezüglicher Vorschlag im gegenständlichen Gesetzesentwurf enthalten ist.

Der Datenschutzrat weist einleitend darauf hin, dass **Straftatbestände, die Angriffe auf Computersysteme (Online Angriffe) und die widerrechtliche Verwendung personenbezogener Daten unter Strafe stellen**, nach geltendem Recht – und auch nach dem vorliegenden Entwurf eines Strafrechtsänderungsgesetzes 2015 – **in mehreren Gesetzen geregelt sind.** Diesbezüglich wird neben den relevanten Regelungen im **StGB (§§ 118a ff)** insbesondere auf **§ 51 DSG 2000** sowie **§§ 10 f des Zugangskontrollgesetzes (ZuKG)**, BGBl. I Nr. 60/2000, hingewiesen.

Diese **Aufsplitterung der einschlägigen Straftatbestände** führt zu terminologischen Problemstellungen sowie zu Fragen des Anwendungsbereiches und des Verhältnisses zwischen den jeweiligen Straftatbeständen. Daneben erscheinen auch die Einordnung von Straftatbeständen als Offizialdelikt (zB § 51 DSG 2000) oder als Ermächtigungsdelikt (wie zT der vorgesehene § 118a StGB) sowie die unterschiedlichen Strafrahmen abstimmungsbedürftig.

In diesem Zusammenhang wird auch von den von der **Strafrechtsexpertin Univ.-Prof. Dr. Susanne Reindl-Krauskopf** veröffentlichten Aufsatz **Cyberstrafrecht im Wandel**, ÖJZ 2015/19, hingewiesen.

Die Bedeutung des Computerstrafrechts wird auch durch die **Beantwortung der parlamentarischen Anfrage betreffend „Internetkriminalität – Strafdelikte durch IT-Medium im Jahr 2014“** (Zahl 3571/J) durch die Bundesministerin für Inneres (3400/AB) ersichtlich, wonach im Bereich der Internetkriminalität im Jahr 2014 vor allem die „widerrechtlichen Zugriffe auf IT-Systeme“ sowie der Tatbestand des „Missbrauchs von Computerprogrammen oder Zugangsdaten“ zugenommen haben. In der Anfragebeantwortung wird zudem ausgeführt, dass aufgrund der derzeitigen Rechtslage im Rahmen der Kriminalprävention verstärkt auf die **Gefahren bei der Nutzung des Internet** und insbesondere von sozialen Medien bei Anfragen an die **Meldestelle** hingewiesen wird, da **ein starker Anstieg bei Tathandlungen mit Identitätsdiebstahl und Erpressungen nach sexuellen Handlungen vor laufender Kamera im Internet verzeichnet werden konnte.**

Im Lichte dieser dargestellten Problemstellungen regt der Datenschutzrat an, dass eine **umfassende, geschlossene Regelung des sogenannten „Computerstrafrechts“ in einem gesonderten Kapitel im StGB** geschaffen wird (zB Computer- und Internetstrafrecht), im dem auch die derzeit noch in materienspezifischen Gesetzen geregelten und zu diesem Bereich gehörigen Straftatbestände sprachlich sowie begrifflich abgestimmt aufgenommen werden.

Weiters müsste aus Sicht des Datenschutzrates berücksichtigt werden, dass durch **neue Technologien und Geschäftsmodelle (Stichworte: „Big Data“ sowie Online Speicherdienste/Cloud)** Daten nicht mehr nur lokal auf dem eigenen Computer gespeichert werden. Es sollte daher ausdrücklich geprüft werden, ob von der im Entwurf weiterverwendeten Definition „**Computersystem**“, die nach § 74 Abs. 1 Z 8 StGB „**sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen“** umfasst, auch diese neuen technischen Entwicklungen umfasst sind.

Der Datenschutzrat regt an, dass in den Erläuterungen ausdrücklich klargestellt werden sollte, welche neuen Technologien unter den Begriff „Computersystem“ fallen.

I. Artikel 1 (Änderung des Strafgesetzbuches):

Zu Z 47 (§ 118a):

Im Hinblick auf den in § 51 DSG 2000 verankerten Straftatbestand der Datenverwendung in Gewinn- oder Schädigungsabsicht, der Berührungspunkte mit § 118a

StGB aufweist, sollten Ausführungen über die Auswirkungen der vorgeschlagenen Änderungen des § 118a auf diese Strafnorm in die Erläuterungen aufgenommen bzw. die Bestimmungen allenfalls angepasst werden.

In diesem Zusammenhang ist darauf hinzuweisen, dass § 51 DSG 2000 (seit der DSG-Novelle 2010, BGBl. I Nr. 133/2009) ein Offizialdelikt darstellt und mit einem Jahr Freiheitsstrafe bedroht ist, während § 118a idF des vorliegenden Entwurfes gemäß dessen Abs. 3 nur mit Ermächtigung des Verletzten zu verfolgen und mit bis zu sechs Monaten (Abs. 1) bzw. im Falle der qualifizierten Begehung (in Bezug auf ein Computersystem, das ein wesentlicher Bestandteil der kritischen Infrastruktur ist [Abs. 2] oder bzw. und im Rahmen einer kriminellen Vereinigung [Abs. 4]) mit bis zu zwei bzw. drei Jahren Freiheitsstrafe zu bestrafen ist.

Werden durch eine Handlung sowohl § 118a Abs. 2 StGB als auch § 51 DSG 2000 verwirklicht (etwa, wenn infolge des Eindringens in ein Computersystem der kritischen Infrastruktur, das ein „widerrechtliches Verschaffen“ von Daten iSd § 51 DSG 2000 darstellt, personenbezogene Daten in Bereicherungs- und Schädigungsabsicht gemäß § 51 DSG 2000 verwendet werden), stellt sich – im Hinblick auf den Subsidiaritätsvorbehalt im vorletzten Halbsatz des § 51 DSG 2000 – insbesondere die Frage, welche Strafnorm anzuwenden ist, wenn eine Ermächtigung zur Verfolgung der Straftat gemäß § 118a Abs. 3 nicht erteilt wird.

Ferner erscheint (aufgrund der Reihenfolge der Absätze) unklar, ob der Ermächtigungsvorbehalt des Abs. 3 auch im Falle einer Qualifikation gemäß Abs. 4 anzuwenden ist; ist dies der Fall, stellt sich auch hier die Frage nach dem Verhältnis zu § 51 DSG 2000.

Ginge man davon aus, dass § 51 DSG 2000 aufgrund der höheren Strafdrohung in § 118a Abs. 2 unabhängig davon verdrängt wird, ob eine Ermächtigung zur Verfolgung gemäß § 118a Abs. 3 erteilt wird, hätte dies ein Datenschutz-Defizit zur Folge, weil der „Verletzte“ iSd Art. 118a Abs. 3 der Zugriffsberechtigte des Computersystems ist (ErlRV 1166 BlgNR 21. GP 25), dh. idR der datenschutzrechtliche Auftraggeber iSd § 4 Z 4 DSG 2000 und nicht jene Person(en), auf die sich die personenbezogenen Daten beziehen (datenschutzrechtlich Betroffene iSd § 4 Z 3 DSG 2000). Diese Problematik ist allerdings insofern nicht neu, als § 51 DSG 2000 idF vor der DSG-Novelle 2010 zwar ebenfalls ein Ermächtigungsdelikt war, der

„Verletzte“ jedoch hier der Betroffene (und nicht – wie im Falle des § 118a Abs. 3 StGB – der Zugriffsberechtigte) war.

Geht man hingegen davon aus, dass § 51 DSG 2000 von § 118a Abs. 2 StGB nur dann verdrängt wird, wenn eine Ermächtigung gemäß Abs. 3 leg.cit. erteilt wird, läge es letztlich in der Hand des Verletzten, zu entscheiden, welche Strafdrohung für die strafbare Handlung zur Anwendung gelangen soll, was Bedenken im Lichte des Art. 7 EMRK aufwirft.

Der Datenschutzrat nimmt zur Kenntnis, dass die informierten Vertreter in der Sitzung des Datenschutzrates zugesichert haben, entsprechende Klarstellungen zur Person des Verletzten bzw. Betroffenen in die Erläuterungen aufzunehmen.

Zu Z 49 (§ 120a):

Mit Abs. 1 Z 2 werden die Bekanntgabe und die Veröffentlichung von Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches einer Person als „fortgesetzte Belästigung“ unter Strafe gestellt.

Bei der Gestaltung dieses Straftatbestandes ist darauf zu achten, dass nur solche Handlungen erfasst werden, bei denen die Verwendung personenbezogener Daten auch datenschutzrechtlich, dh. nach den Bestimmungen des DSG 2000 sowie allfälliger materienspezifischer Datenschutzvorschriften, unzulässig ist.

So ist etwa zu anzumerken, dass nach dem Wortlaut der vorgeschlagenen Bestimmung die fortgesetzte Belästigung in einer Weise erfolgen muss, „die geeignet ist, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen“. Dabei wird ausschließlich auf die Zumutbarkeit im Hinblick auf die in ihrer Lebensführung beeinträchtigte Person abgestellt; aus den Erläuterungen ergibt sich, dass die Beurteilung der Unzumutbarkeit von den „konkreten Umständen im Einzelfall“ abhängt und eine solche im Falle des Abs. 1 Z 2 nur angenommen werden kann, wenn die Bekanntgabe oder Veröffentlichung „(objektiv) geeignet ist, das Opfer bloßzustellen“.

Nach den Bestimmungen des DSG 2000 – die hier insofern maßgeblich sind, als sie die verpflichtenden unionsrechtlichen Vorgaben der Richtlinie 95/46/EG umsetzen – ist die Verwendung von personenbezogenen Daten hingegen u.a. dann zulässig, wenn überwiegende Interessen an der Verwendung der Daten bestehen (vgl. § 8

Abs. 1 Z 4 DSG 2000 bzw. Art. 7 lit. f der Richtlinie 95/46/EG); die Beurteilung hängt daher von einer Abwägung zwischen den Interessen des Betroffenen und des Auftraggebers der Datenverwendung ab, wohingegen § 120a Abs. 1 des Entwurfes ausschließlich auf die Interessenlage beim Betroffenen abstellt.

Zur Vermeidung von Widersprüchen zwischen datenschutzrechtlicher und strafrechtlicher Beurteilung der Zulässigkeit einer Bekanntgabe oder Veröffentlichung von Tatsachen oder Bildaufnahmen wird empfohlen, in den Erläuterungen klarzustellen, dass eine datenschutzrechtlich zulässige Verwendung personenbezogener Daten nicht unzumutbar iSd § 120a sein kann.

Im Hinblick auf den in Abs. 1 Z 2 verwendeten Begriff der „Zustimmung“ sollte klargestellt werden, ob es sich um eine datenschutzrechtliche Zustimmung gemäß § 4 Z 14 DSG 2000 handelt.

Ferner wird angeregt, in den Erläuterungen darauf hinzuweisen, dass der Begriff der „Bildaufnahmen“ auch Videoaufnahmen umfasst.

Ziel dieser Bestimmung ist daher der **strafrechtliche Schutz der Persönlichkeitsrechte** einer Person.

Der Datenschutzrat begrüßt grundsätzlich diese vorgesehene Regelung.

Zu Z 204 (§ 301 Abs. 3):

Der Tatbestand des § 301 Abs. 3 (Verbotene Veröffentlichung) umfasst u.a. Mitteilungen über den Inhalt von Ergebnissen aus einer Auskunft über Vorratsdaten; die Bestimmungen des Telekommunikationsgesetzes 2003, der Strafprozeßordnung 1975 und des Sicherheitspolizeigesetzes über die Vorratsdatenspeicherung wurden jedoch mit BGBl. I Nr. 44/2014 (Kundmachung des am 27. Juni 2014 verkündeten Erkenntnisses des Verfassungsgerichtshofes, G 47/2012 ua.) mit Ablauf des 30. Juni 2014 aufgehoben.

Aus datenschutzrechtlicher Sicht erscheint es zwar geboten, die verbotene Veröffentlichung von Vorratsdaten auch weiterhin unter Strafe zu stellen, soweit vor der Aufhebung der gesetzlichen Bestimmungen ermittelte Vorratsdaten betroffen sein könnten; im Hinblick auf den Wegfall insbesondere der Begriffsbestimmung für die „Auskunft über Vorratsdaten“ (§ 134 Z 2a StPO idF BGBl. I Nr. 35/2012) wäre jedoch zu prüfen, ob diese Strafnorm im Lichte des Art. 7 EMRK noch ausreichend bestimmt ist.

II. Artikel 2 (Änderung des Suchtmittelgesetzes):

Zu Z 1 (§ 13 Abs. 2a):

Mit dem vorgeschlagenen Abs. 2a werden Behörden und öffentliche Dienststellen verpflichtet, einen ihnen bekannt gewordenen Anfangsverdacht bestimmter Suchtgiftdelikte anstelle einer Strafanzeige (§ 78 StPO) der Bezirksverwaltungsbehörde als Gesundheitsbehörde mitzuteilen.

Da eine solche Mitteilung nach den Voraussetzungen dieser Bestimmung Gesundheitsdaten, nämlich die Information über den Gebrauch von Suchtgift durch die Person selbst oder durch eine andere Person, umfasst, handelt es sich dabei um eine Verwendung (Übermittlung) sensibler, dh. besonders schutzwürdiger Daten (§ 1 Abs. 2 zweiter Satz bzw. § 4 Z 2 DSG 2000). Darüber hinaus sind diese aufgrund des Bezuges zu einer Straftat auch als strafrechtsrelevante Daten zu qualifizieren. Solche Daten unterliegen gemäß Art. 8 der Richtlinie 95/46/EG besonderem Schutz und dürfen ausschließlich zu den in dieser Bestimmung taxativ angeführten Zwecken verwendet werden (vgl. auch § 1 Abs. 2 zweiter Satz sowie § 8 DSG 2000). Ferner muss die Verwendung der Daten im Hinblick auf den jeweiligen Verwendungszweck notwendig und verhältnismäßig sein.

Ob diese datenschutzrechtlichen Voraussetzungen im Hinblick auf § 13 Abs. 2a des Entwurfes vorliegen, ist vornehmlich vom do. Bundesministerium zu beurteilen. Es wird jedoch grundsätzlich empfohlen, im Gesetzestext klar festzulegen, zu welchen Zwecken die übermittelten Daten verwendet werden dürfen. In diesem Zusammenhang wird darauf hingewiesen, dass eine Weiterverwendung dieser Informationen durch die Bezirksverwaltungsbehörde zu anderen Zwecken – mögen sie auch zu deren Aufgabenbereich zählen (zB Gewerbebehörde) – aus datenschutzrechtlicher Sicht eine eigene Übermittlung iSd § 4 Z 12 DSG 2000 darstellt, die einer gesonderten Rechtsgrundlage bedarf (!).

Fraglich ist aber, ob die verpflichtende Mitteilung gemäß § 13 Abs. 2a SMG – die Gesundheitsdaten (Suchtgiftmissbrauch) umfasst – in jedem Fall einem der in Art. 8 der RL 95/46/EG dargelegten Fälle zugeordnet werden kann. Der Ausnahmetatbestand des Art. 8 Abs. 3 (Gesundheitsvorsorge) dürfte etwa nicht zum Tragen kommen, wenn die Straftat ausschließlich für den persönlichen Gebrauch eines anderen zum Tragen kommt; ferner hat diese Bestimmung vorwiegend die Verwendung durch Ärzte und medizinisches Personal im Auge (vgl. auch § 9 Z 12

DSG 2000). Soweit Art. 8 Abs. 4 der RL 95/46/EG weitere Ausnahmen durch nationale Vorschriften erlaubt, stellt sich die Frage, ob hier ein „wichtiges öffentliches Interesse“ iSd § 9 Z 3 DSG 2000 vorliegt, das in jedem Fall die Übermittlung sensibler Daten an die Bezirksverwaltungsbehörde als Gesundheitsbehörde rechtfertigt.

27. April 2015
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt