

DATENSCHUTZ

KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Auskunft

**Ist hier wirklich nichts? Besonderheiten
der „Negativauskunft“**

Reinhard Hübelbauer

**Strafrechtliche Folgen eines Missbrauchs
des Auskunftsrechts**

Célia Chausse und Georg Kudrna

**Verfahrensrechtliche Aspekte einer Meldung
nach Art 33 DSGVO**

Andreas Zavadil und Christina Maria Schwaiger

Checkliste: Nutzungsrichtlinie für IKT

Markus Oman und Siegfried Gruber

Ist das Modell „Daten gegen gratis“ wirklich fair?

Interview mit Clemens Appl, Donau-Uni Krems

Praxisbeitrag: Datenschutz in den Alltag bringen

Renate Grabinger

Immaterieller Schadenersatz ohne Schaden?

Thomas Schweiger

Célia Chausse/Georg Kudrna

Fachkordinatorin BMDW/Rechtsanwaltsanwarter bei Rohregger Scheibner Rechtsanwalt GmbH

Strafrechtliche Folgen eines Missbrauchs des Auskunftsrechts (Teil 1)

Widerrechtliches Verschaffen; Benutzen; Tauschung. Kann jemand, der ein Auskunftsbegehren stellt und sich dabei als jemand anderer ausgibt, strafrechtlich belangt werden? Teil 1 des Beitrags konzentriert sich auf jene Falle, in denen der Verantwortliche dem privaten Sektor zugehort. Teil 2 behandelt die Falle, wo der Verantwortliche dem ublichen Bereich¹ angehort.²

Einleitung

Das Strafgesetzbuch (StGB) sieht verstreut Straftatbestande vor, die strafbare Handlungen iZm Daten ahnden.³ Auch das DSGVO sieht in § 63⁴ (Datenverarbeitung in Gewinn- oder Schadigungsabsicht) einen gerichtlichen Straftatbestand vor.⁵ Doch besteht durch diese – oder eine andere – Norm eine strafgerichtliche Sanktionierung im Fall eines widerrechtlichen Verschaffens von personenbezogenen Daten durch ein missbrauchliches Auskunftsbegehren.⁶ Und wird dem Spannungsverhaltnis zwischen dem Ausbau der Betroffenenrechte durch die DSGVO und der Sanktionierung im Fall eines Missbrauchs des Datenschutzes genugend Rechnung getragen?

Datenverarbeitung in Gewinn- oder Schadigungsabsicht (§ 63 DSGVO)

Denkbar erscheint, dass jemand, der sich widerrechtlich personenbezogene Daten verschafft, indem er sich missbrauchlich im Rahmen eines Auskunftsbegehrens als Betroffener ausgibt, den Straftatbestand des § 63 DSGVO⁷ erfullt. Nach § 63 DSGVO macht sich (gerichtlich) strafbar, wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmaig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs 1 DSGVO gewahrleisteten Anspruch (auf Datenschutz)⁸ zu schadigen, personenbezogene Daten, die ihm ausschlielich auf Grund seiner berufsmaigen Beschaftigung anvertraut oder zuganglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benutzt, einem anderen zuganglich macht oder veroffentlicht, obwohl der Betroffene an diesen Daten ein schutzwurdiges Geheimhaltungsinteresse⁹ hat. § 63 DSGVO soll das Grundrecht auf Datenschutz gem § 1 DSGVO schutzen.¹⁰ Das darin umfasste Recht auf Geheimhaltung personenbezogener Daten bzw das damit einhergehende Recht auf „informationelle Selbstbestimmung“¹¹ sind das primar geschutzte Rechtsgut.¹²

Widerrechtliches Verschaffen

Voraussetzung des Tatbestands des § 63 DSGVO ist, dass die schutzwurDIGen personenbezogenen Daten dem Tater entweder

- aufgrund seiner berufsmaigen Beschaftigung anvertraut oder zuganglich geworden sind, oder
- er sich sie – (auch) auerhalb der Arbeitswelt – widerrechtlich verschafft hat.¹³

Verschaffen bedeutet, dass der Tater die Daten durch aktives Tun in seine Verfugungsmacht bringen muss.¹⁴ Darunter fallt jegliche **proaktive Handlung**, die unmittelbar oder mittelbar zu einem unrechtmaigen Erlangen der Daten fuhrt. Daher liegt ein widerrechtliches Verschaffen vor, wenn jemand missbrauchlich ein Auskunftsbegehren stellt, ohne hierzu berechtigt zu sein, und hierdurch widerrechtlich Daten erlangt.¹⁵

Nur eine aktive Handlung kann zu einem widerrechtlichen Verschaffen fuhren.

Der Verschaffungsakt muss auerdem widerrechtlich sein. Die **Widerrechtlichkeit** kann sich aus der gesamten Rechtsordnung ergeben.¹⁶ Bei einem missbrauchlichen Auskunftsbegehren ergibt sich die Widerrechtlichkeit bereits aus Art 15 DSGVO, der ausschlielich der betroffenen Person das Auskunftsrecht einraumt.¹⁷

Benutzen

Als Tathandlung des § 63 DSGVO kommen das Selbst-Benutzen, Einem-anderen-Zuganglichmachen oder Veroffentlichen der Daten in Frage. Differenziert beurteilt wird in der Lit va die Frage, was als „Benutzen“ iSd § 63 DSGVO zu qualifizieren ist. Nach Ansicht *Bergauers* ist unter Benutzen das „Verarbeiten von Daten“ nach datenschutzrechtlicher Terminologie¹⁸ zu verstehen. Das hatte zur Folge, dass auch die Spei-

cherung oder sonstige Verarbeitung ohne Auenwirkung widerrechtlich erlangter Daten das objektive Tatbild des § 63 DSGVO erfullen (konnten).¹⁹ Insb²⁰ *Salimi* hingegen vertritt die Ansicht, dass nur solche Tathandlungen in Frage kommen, welche eine Verletzung des Geheimhaltungsinteresses bewirken, was lediglich bei Handlungen

¹ Zur Abgrenzung siehe zB *Gerhartl*, Besonderheiten des ublichen Bereichs, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 361. ² Eine Erortderung moglicher Delikte, wenn weitere Tatbestandselemente hinzukommen (zB Betrug, Urkundenfalschung), wurde den Rahmen des Beitrags berschreiten und erfolgt daher nicht. Daruber hinaus konzentriert sich der Beitrag auf gerichtliche Straftatbestande. ³ StGB: § 126 a (Schutz von Daten mit Vermogenswert vor Beschadigung oder Unterdruckung); §§ 123, 124 (Schutz vor dem Ausspionieren von Daten, die ein Betriebs- oder Geschäftsgeheimnis darstellen); § 118 a (Zugangsverschaffung zu einem fremden Computersystem); §§ 119 ff (Strafbare Handlungen iZm der Benutzung von Abhorvorrichtungen und Spionagehandlungen); §§ 121 f (Geheimnisschutz); § 225 a (Falschung oder Verfalschung von Daten). Werden rechtswidrig erlangte Daten zur unrechtmaigen Bereicherung verwendet, liegt uU ein Datenbetrug gem § 147 Abs 1 Z 1 3. Fall StGB vor. Werden Daten zur Beeinflussung eines Datenverarbeitungsprozesses verwendet, wird uU § 148 a StGB erfullt. § 107 a StGB (Stalking) beinhaltet einen Fall, in dem personenbezogene Daten zur Bestellung von Waren oder Dienstleistungen oder zur Veranlassung der Kontaktaufnahme durch Dritte verwendet werden; siehe *Salimi* in *Hoppel/Ratz*, WK² DSGVO § 51 Rz 2 (Stand 1. 5. 2012, rdb). ⁴ BGBl I 2017/120. ⁵ Nach *Salimi* handelt es sich um den umfassendsten strafrechtlichen Schutz vor einer rechtswidrigen Verwendung personenbezogener Daten, vgl *Salimi* in *Hoppel/Ratz*, WK² DSGVO § 51 Rz 2 (Stand 1. 5. 2012, rdb). ⁶ Zum Recht auf Auskunft im Allgemeinen siehe *Haidinger* in *Knyrim*, DatKomm Art 15 Rz 1 ff mwN. ⁷ Die Bestimmung entspricht § 51 DSGVO 2000, die Erlaut sprechen von einer „unveranderten Regelung“; ErlautAB 1761 BlgNR 25 GP 29; *Illbauer* in *Knyrim*, DatKomm Art 84 Rz 22. ⁸ Zum Grundrecht auf Datenschutz siehe *Lachmayer* in *Knyrim*, DatKomm Art 1 Rz 32, 51 ff mwN. ⁹ Vgl *Pradler*, Datenmissbrauch in der ublichen Verwaltung (2001) 164. ¹⁰ *Salimi* in *Hoppel/Ratz*, WK² DSGVO § 51 Rz 2 (Stand 1. 5. 2012, rdb). ¹¹ *Bergauer*, Der Handel mit Patientendaten – eine (datenschutzrechtliche) Straftat? *JZ* 2013, 959; *Bull*, Notwendigkeit und Grenzen des Datenschutzes im Bereich der inneren Sicherheit, in *BMI* (Hrsg), Sicherheit und Grundrechtsschutz (2019) 91. ¹² *Salimi* in *Hoppel/Ratz*, WK² DSGVO § 51 Rz 3 (Stand 1. 5. 2012, rdb) mwN. ¹³ *Bergauer*, *JZ* 2013, 960. ¹⁴ *Salimi* in *Hoppel/Ratz*, WK² DSGVO § 51 Rz 21 (Stand 1. 5. 2012, rdb) mwN; *Salimi*, Zahnloses Cyberstrafrecht? Eine Analyse der gerichtlichen Straftatbestande zum Daten- und Geheimnisschutz, *JZ* 2012, 1002. ¹⁵ Lediglich eine vollig passive Verhaltensweise ist nicht ausreichend, vgl *Salimi* in *Hoppel/Ratz*, WK² DSGVO § 51 Rz 21 (Stand 1. 5. 2012, rdb) mwN; *Salimi*, *JZ* 2012, 1002. ¹⁶ Diesbezuglich kommen va strafrechtliche Normen in Frage, aber auch die Verletzung einer Verwaltungs(strabestimmung (zB § 62 DSGVO) oder zivilrechtswidriges Verhalten konnen zu einem widerrechtlichen Erlangen fuhren; *Salimi* in *Hoppel/Ratz*, WK² DSGVO § 51 Rz 22 ff (Stand 1. 5. 2012, rdb). ¹⁷ Siehe hierzu auch *Haidinger* in *Knyrim*, DatKomm Art 15 Rz 11. ¹⁸ *Bergauer* zieht die damalige Legaldefinition des § 4 Z 9 DSGVO 2000 heran, die nicht mehr in Kraft ist. Nimmehr ist auf die Begriffsbestimmung des Art 4 Z 2 DSGVO abzustellen, wonach als Verarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgefuhrte Vorgang oder jede solche Vorgangsreihe iZm personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veranderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch bermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknupfung, die Einschrankung, das Loschen oder die Vernichtung, zu verstehen ist. ¹⁹ *Bergauer*, *JZ* 2013, 960 ff. ²⁰ Auch *Thiele* ist der Ansicht, dass nicht samtliche Falle des „Verarbeitens“ darunter fallen, vgl *Thiele*, SbgK Vorbem §§ 118 ff Rz 61.

mit einer gewissen **Außenwirkung** möglich wäre.²¹ Das bloß interne Speichern, das Löschen oder das Vervielfältigen der Daten ohne nach außen hin gerichteten Akt könne nicht zur Verletzung von Geheimhaltungsinteressen führen, sodass diese Handlungen nicht tatbildlich wären.²²

UE ist zwar ein „Benützen“ iSd § 63 DSGVO nicht völlig gleichzusetzen mit jeder Verarbeitung von Daten iSd Art 4 Z 2 DSGVO. Denn wäre dies die Intention des Gesetzgebers gewesen, so hätte er auch den Begriff des Verarbeitens in § 63 DSGVO aufgenommen. Nicht erforderlich für ein Benützen erscheint uE jedoch, dass zwingend eine Tathandlung mit Außenwirkung (über den Täter hinaus) erfolgen muss. Das Grundrecht auf Datenschutz kann auch bereits durch das widerrechtliche Verschaffen der Daten verletzt sein. Wenn der Täter aus den widerrechtlich erlangten Daten Informationen erhält und diese – in welcher Form auch immer – **verwertet**, dann **benützt** er die Daten iSd § 63 DSGVO. Eine **Außenwirkung ist hierfür nicht erforderlich**.²³ Liest bspw der Täter die erlangten Daten, so liegt bereits eine Verletzung des Grundrechts auf Datenschutz vor. Als Benützen iSd § 63 DSGVO ist sohin uE jegliche Handlung bzw Verwertung iZm den widerrechtlich erlangten Daten zu verstehen, wodurch das Grundrecht auf Datenschutz verletzt wird, und zwar gleichgültig, ob es zu einer unmittelbaren oder mittelbaren Außenwirkung kommt oder auch nicht.²⁴

Vorsatz

Der Täter muss über den Tatbestandsvorsatz hinaus entweder Vorsatz auf unrechtmäßige Bereicherung haben oder in der Absicht handeln, den Betroffenen in dessen durch § 1 Abs 1 DSGVO gewährleisteten Anspruch zu schädigen.²⁵ Dem Täter muss es somit darauf ankommen, dass das Opfer im Anspruch auf Geheimhaltung geschädigt wird.²⁶ Nicht ausreichend erscheint uE die Absicht, einem anderen einen Nachteil in Form eines Gefühlsschaden zuzufügen.²⁷ Eventualvorsatz reicht nicht aus.²⁸ Diese Schwelle der subjektiven Tatseite wird wohl nicht bei jedem missbräuchlichen Auskunftsbegehren vorliegen und eine Strafbarkeit wird in solchen Fällen ausscheiden.

Täuschung (§ 108 StGB)

Doch sogar, wenn man für ein „Benützen“ iSd § 63 DSGVO ein **enges** Begriffsverständnis vertreten würde, scheinen strafrechtliche

Folgen für jemanden, der „nur“ widerrechtlich personenbezogene Daten erhält, indem er sich wahrheitswidrig als Betroffener ausgibt und daher über seine wahre Identität täuscht, aber die erhaltenen Daten nicht in irgendeiner Weise nach außen trägt oder mit Außenwirkung benützt, keineswegs ausgeschlossen. Denkbar erscheint eine Täuschung iSd § 108 StGB, die der begeht, der einem Anderen in seinen Rechten dadurch absichtlich einen Schaden zufügt, dass er ihn oder einen Dritten durch Täuschung über Tatsachen zu einer Handlung, Duldung oder Unterlassung verleitet.

§ 108 StGB erfordert einen (**konkreten**) **Schaden** in Individualrechten.²⁹ Nach der von *Soyer/Schumann* vertretenen Ansicht³⁰ sind Beeinträchtigungen des Grundrechts auf Datenschutz kein Schaden iSd § 108 Abs 1 StGB. Sie begründen ihre Ansicht damit, dass ausreichender strafrechtlicher Schutz des Grundrechts auf Datenschutz durch andere Bestimmungen³¹ gewährleistet sei. Gerade wenn man aber der Ansicht *Salimis* folgen würde, wonach ein Benützen iSd § 63 DSGVO erst vorliegen kann, wenn eine gewisse Außenwirkung besteht, würde jedenfalls kein ausreichender strafrechtlicher Schutz des Grundrechts auf Datenschutz bestehen. Wie erwähnt, wird das Grundrecht auf Datenschutz des Opfers bereits dadurch verletzt, dass der Täter rechtswidrig personenbezogene Daten erhält und auf diese Zugriff hat.

Die Verletzung in einem Persönlichkeitsrecht ist ein Schaden iSd Täuschung.

Der OGH bejaht das Vorliegen eines Schadens iSd § 108 StGB bei einer Verletzung in Persönlichkeitsrechten.³² Diesem Standpunkt folgend scheint es nur schlüssig, auch eine Verletzung im Grundrecht auf Datenschutz als Schaden iSd § 108 StGB zu qualifizieren.

Die für § 108 StGB erforderliche Tathandlung der Täuschung liegt jedenfalls vor, wenn der Täter sich fälschlicherweise als Betroffener ausgibt und Auskunft begehrt sowie diese auch erhält.³³ Auch bei der Täuschung ist eine Absicht des Täters, den Betroffenen absichtlich in seinen Rechten – konkret in seinem Grundrecht auf Datenschutz – zu schädigen, erforderlich.

Ergebnis

Wer sich vorsätzlich wahrheitswidrig als Betroffener iSd Art 1 Z 1 DSGVO ausgibt, um sich widerrechtlich über ein Auskunftsbegehren personenbezogene Daten zu verschaffen, und dabei die Absicht hat, das Opfer in seinem Grundrecht auf Datenschutz zu schädigen, macht sich gerichtlich strafbar. Als Straftatbestand kommt insb § 63 DSGVO in Frage. Ist dieser Straftatbestand nicht erfüllt, ist eine Täuschung gem § 108 StGB denkbar. Bei beiden Delikten ist jedoch erforderlich, dass der Täter (auch) die Absicht hat, den Betroffenen in seinem Grundrecht auf Datenschutz zu schädigen.

Der Ansicht, dass es in Österreich (noch) keinen strafrechtlichen Schutz vor „Datendiebstahl“ per se gebe,³⁴ kann uE nicht gefolgt werden. Es mag sein, dass die in erster Linie in Frage kommenden Straftatbestände (§ 63 DSGVO, § 108 StGB) in der Praxis beinahe totes Recht sind, doch ändert dies nichts an gegenwärtig ausreichenden Strafbestimmungen.³⁵ Es liegt sohin (nur) an der Praxis, das angeblich tote Recht in einem so lebendigen und wichtigen Bereich wie dem Datenschutzrecht zum Leben zu erwecken. Gerade in den Bereichen Datenschutz und Cybercrime wird es geboten sein, Verletzungen des Grundrechts auf Datenschutz – va auch mit den vorhandenen Normen – zu verhindern.³⁶

Dako 2019/57

²¹ *Salimi* in Höpfel/Ratz, WK² DSGVO § 51 Rz 38, 42 (Stand 1. 5. 2012, rdb); *Salimi*, ÖJZ 2012, 1002. ²² *Salimi* in Höpfel/Ratz, WK² DSGVO § 51 Rz 45 (Stand 1. 5. 2012, rdb); *Salimi*, ÖJZ 2012, 1002; *Thiele*, SbgK Vorbem §§ 118 ff Rz 61. Nach *Pradler* kann eine Speicherung allein nicht den Straftatbestand erfüllen; *Pradler*, Datenmissbrauch (2001) 167. ²³ In diese Richtung auch *Pradler*, Datenmissbrauch 165. ²⁴ Vgl auch LG Salzburg 29. 4. 2011, 49 BI 17/11v justT 2011/89, 185. ²⁵ *Salimi* in Höpfel/Ratz, WK² DSGVO § 51 Rz 55 (Stand 1. 5. 2012, rdb). Vor Inkrafttreten der DSGVO-Nov 2010 war es ausreichend, wenn der Täter die Absicht hatte, einem Dritten einen „Nachteil“ zuzufügen, damit erfasst waren alle Formen von Nachteilen; vgl *Salimi* in Höpfel/Ratz, WK² DSGVO § 51 Rz 60 (Stand 1. 5. 2012, rdb). ²⁶ *Salimi* in Höpfel/Ratz, WK² DSGVO § 51 Rz 62 (Stand 1. 5. 2012, rdb. at). ²⁷ Vgl *Thiele*, SbgK Vorbem §§ 118 ff Rz 61. ²⁸ *Soyer/Schumann* in Höpfel/Ratz, WK² StGB § 108 StGB Rz 22 (Stand 1. 5. 2016, rdb.at) mwN. ²⁹ *Soyer/Schumann* in Höpfel/Ratz, WK² StGB § 108 StGB Rz 9 (Stand 1. 5. 2016, rdb.at). ³⁰ *Soyer/Schumann* in Höpfel/Ratz, WK² StGB § 146 (Stand 1. 3. 2019, rdb.at) Rz 17 ff mwN. ³¹ *Salimi*, ÖJZ 2012, 1002. ³² *AA* *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015, 115. ³³ Vgl *Salimi*, ÖJZ 2012, 1003.

Über die Autorin und den Autor

Mag. Célia Chausse ist Fachkoordinatorin der Sektion EU und internationale Marktstrategien im Bundesministerium für Digitalisierung und Wirtschaftsstandort und als solche auch für Datenschutz zuständig. E-Mail: Celia.Chausse@bmdw.gv.at

Mag. Georg Kudrna ist Rechtsanwaltsanwärter bei Rohregger Scheibner Rechtsanwälte GmbH. Zu seinen Schwerpunkten zählen Wirtschafts- und Cyberstrafrecht. E-Mail: georg.kudrna@rwk.at

Hinweis

Teil 2 des Beitrags erscheint in der nächsten Ausgabe der Dako und behandelt den öffentlichen Bereich.