Datenschutz im Strafverfahren

Durch Inkrafttreten der DSGVO[1] Mitte 2016 ist das Datenschutzrecht als eigene Rechtsmaterie (noch mehr) in den Mittelpunkt des juristischen und öffentlichen Interesses gerückt. Dies hatte den durchaus positiven Effekt, dass zahlreiche Unternehmen und auch öffentliche Stellen seither wesentlich sensibler mit personenbezogenen Daten umgehen.
Wenig Beachtung in Wissenschaft und Praxis fanden die zeitgleich eingeführten Änderungen im Strafprozess: Durch Änderungen in der StPO mit BGBl I 2018/32 als auch des DSG[2] mit BGBl I 2018/24 wurden Betroffenenrechte in Bezug auf in Strafverfahren verarbeitete personenbezogene Daten präzisiert. Gerade aufgrund deren gesetzlicher Funktion, eben gerade auch personenbezogene Daten zu ermitteln und zu verwerten, verdient der rechtliche Rahmen eine genauere Betrachtung.

Deskriptoren: Datenschutz im Strafverfahren, Privatsphäre, Familienleben, Löschung, Löschungsrecht, Berichtigung, Einsichtsrecht bei Kriminalpolizei, Geheimhaltung personenbezogener Daten.

Normen: DSGVO; DSRL-PJ; DSG; StPO; GOG; StAG.

Von Alexander Stücklberger und Georg Kudrna

1. Anwendbare datenschutzrechtliche Bestimmungen im Strafverfahren

Es stellt sich zu Beginn die Frage, welche unionsrechtlichen und nationalen Bestimmungen in Zusammenhang mit Datenschutz im (österreichischen) Strafprozess[3] Anwendung finden.

1.1. DSGVO

Grundsätzlich ist die DSGVO anwendbar, wenn personenbezogene Daten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen, soweit keiner der in Art 2 Abs 2 bis 4 DSGVO angeführten Ausnahmetatbestände zutreffen.[4] Für Strafverfahren kommt der Ausnahmetatbestand des Art 2 Abs 2 lit d DSGVO zur Anwendung. Dieser legt fest, dass die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden findet, wenn die Verarbeitung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit erfolgt. Diese Verarbeitungen werden unionsrechtlich von einer eigenen Richtlinie geregelt.[5] Denkbar wäre ein Anwendungsbereich der DSGVO im Bereich des Strafverfahrens (nur) dann, wenn die Kriterien für die Anwendung der Datenschutz-Richtlinie für den Bereich Justiz und Inneres ("DSRL-PJ")[6] nicht vorliegen.

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
[2] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), StF: BGBl I 1999/165/ idgF.
[3] Wenn in diesem Beitrag von Strafprozess gesprochen wird, ist damit das Verfahren nach der StPO gemeint.
[4] *Heißl* in *Knyrim,* DatKomm, Art 2 Rz 2 f (Stand Februar 2019).
[5] ErwGr 19 DSGVO.
[6] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher

1.2. DSRL-PJ

Die DSRL-PJ wurde gleichzeitig mit der DSGVO verhandelt und schließlich auch beschlossen. Sie ersetzt den im Rahmen der dritten Säule erlassenen Rahmenbeschluss 2008/977/JI aus dem Jahr 2008.[7] DSGVO und DSRL-PJ sind eng aufeinander abgestimmt und ergänzen sich gegenseitig. Dies entspricht dem Ziel der Schaffung eines unionsweit einheitlichen, möglichst lückenlosen Datenschutzrechtsrahmens für alle Sachverhalte, die die Verwendung personenbezogener Daten betreffen und in den Anwendungsbereich des Unionsrechts fallen.[8] Die Abgrenzung dieser beiden Rechtsquellen erfolgt durch den bereits erwähnten Art 2 Abs 2 lit d DSGVO.[9] In den Anwendungsbereich der DSRL-PJ (und damit nicht in den Anwendungsbereich der DSGVO) fallen sowohl präventive als auch repressive Verarbeitungsvorgänge. Es fallen daher nicht nur Verarbeitungsvorgänge der StPO und des StVG darunter, sondern auch nach dem SPG.[10]

1.2.1. Anwendungsbereich

Wie die DSGVO gilt die DSRL-PJ für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.[11] Die DSRL-PJ gilt für die Verarbeitung personenbezogener Daten durch *die zuständigen Behörden zu den Zwecken* der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.[12]

Als zuständige Behörden kommen insbesondere jene staatlichen Behörden in Betracht, die mit Aufgaben im Strafverfolgungsbereich betraut sind. Dabei handelt es sich um die Gerichte, Staatsanwaltschaften, Finanzstrafbehörden, Sicherheitsbehörden sowie sonstige staatliche Behörden, die mit der Erfüllung von Aufgaben im Strafverfolgungsbereich betraut sind.[13] Daneben kommen als "zuständige Behörde" iSd DSRL-PJ auch Private in Betracht, denen die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für Richtlinienzwecke übertragen wurden. In Österreich ist dies aus verfassungsrechtlichen Gründen jedoch ausgeschlossen.[14]

Die *Richtlinienzwecke* umfassen neben dem Bereich der öffentlichen Sicherheit den gesamten Bereich der Strafverfolgung sowie der Strafvollstreckung.[15] Dazu zählen insbesondere Ermittlungshandlungen der Strafverfolgungsbehörden, Datenverarbeitungen in Zusammenhang mit Strafverfahren sowie

---

Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

[7] *Heißl* in *Knyrim,* DatKomm, Art 2 Rz 79 (Stand Februar 2019).

[8] *Dörnhöfer*, Datenschutz im Strafverfolgungsbereich: Schnittstellen und Abrenzungsfragen, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 401.

[9] *Heißl* in *Knyrim,* DatKomm, Art 2 Rz 80 (Stand Februar 2019).

[10] *Heißl* in *Knyrim,* DatKomm, Art 2 Rz 81 (Stand Februar 2019) mwN.

[11] Art 2 Abs 2 DSRL-PJ.

[12] Art 1 Abs 1, Art 2 Abs 1 DSRL-PJ.

[13] Art 3 Z 7 DSRL-PJ.

[14] VfSlg 14.473/1996, 16.400/2001; *Dörnhöfer*, Datenschutz in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 402.

[15] Art 1 Abs 1 DSRL-PJ.

Datenverarbeitungen im Zusammenhang mit der Vollstreckung von Strafen. Nicht unter die Richtlinienzwecke fällt die Justizverwaltung, welche sohin der DSGVO unterliegt.[16] Der Bereich der öffentlichen Sicherheit ist vom Anwendungsbereich der DSRL-PJ soweit umfasst, als ein Zusammenhang mit der Prävention von Straftaten besteht.[17] Polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht, fallen in den Anwendungsbereich der DSRL-PJ. In bestimmten Fällen kann ein polizeilicher Einsatz teils in den Anwendungsbereich der DSGVO, teils in den Anwendungsbereich der DSRL-PJ fallen, etwa wenn zunächst kein Konnex mit einer Straftat besteht, später jedoch ein Einschreiten zur Verhinderung bzw Verfolgung von Straftaten erforderlich wird.[18]

1.2.2. Anwendbarkeit der DSGVO bei Überschreiten des Anwendungsbereichs

Aufgrund der ausdrücklichen Bezugnahme auf die zuständige Behörde fällt eine offensichtlich rechtsmissbräuchliche Datenverarbeitung über die Befugnis und somit über die Zuständigkeit einer Behörde hinaus sehr wohl unter die DSGVO.[19] Datenverarbeitungen einer zuständigen Behörde zu nicht unter die DSRL-PJ fallende Aufgaben sind ebenfalls nach der DSGVO zu beurteilen.[20] Verarbeitet sohin eine Strafverfolgungsbehörde personenbezogene Daten ohne Rechtsgrundlage und ohne einen legitimen Zweck, würde die DSGVO hier unmittelbar Anwendung finden. In einem solchen Fall stehen der betroffenen Person daher wohl auch die unmittelbar anwendbaren Rechte der DSGVO (Auskunftsrecht, Löschungsrecht, etc) vollumfassend zu.

1.2.3. Materielle Unterschiede zwischen DSGVO und DSRL-PJ

Die Datenschutzniveaus von DSGVO und DSRL-PJ unterscheiden sich. Die DSRL-PJ erlaubt vergleichsweise schwerwiegende Eingriffe in das Grundrecht auf Datenschutz der betroffenen Person und sieht verschiedene Einschränkungen im Bereich der Transparenz, der Auskunftsrechte und der Informationspflichten vor. Begründet wird dies mit den besonderen Bedürfnissen im Strafverfolgungsbereich. Die Verarbeitung personenbezogener Daten in der Strafverfolgung erfolgt im Regelfall zum Schutz besonders wichtiger öffentlicher Interessen, nämlich der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie dem Schutz der Rechte und Freiheiten anderer. Transparenzverpflichtungen in einem Ausmaß, wie sie in der DSGVO vorgesehen sind, könnten die Tätigkeit der Strafverfolgungsbehörden teilweise behindern oder sogar vereiteln.[21] Die DSRL-PJ sieht jedoch im Gegenzug eine konkretere gesetzliche Determinierung von Eingriffen und eine engere Zweckbindung vor.[22] Nach der DSRL-PJ bestehen im Vergleich zur DSGVO insbesondere folgende Besonderheiten:[23]

---

[16] *Dörnhöfer*, Datenschutz in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 404.
[17] *Dörnhöfer*, Datenschutz in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 405.
[18] *Dörnhöfer*, Datenschutz in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 405.
[19] *Heißl* in *Knyrim,* DatKomm, Art 2 Rz 85 (Stand Februar 2019); *Ennöckl* in *Sydow,* Europäische Datenschutzgrundverordnung, Art 2 Rz 15.
[20] *Heißl* in *Knyrim,* DatKomm, Art 2 Rz 85 (Stand Februar 2019).
[21] *Dörnhöfer*, Datenschutz in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 401.
[22] *Dörnhöfer*, Datenschutz in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 402.
[23] *Dörnhöfer*, Datenschutz in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 402.

● Jede Datenverwendung iSd DSRL-PJ bedarf einer gesetzlichen Grundlage.[24] Überwiegendes berechtigtes Interesse[25] ist keine ausreichende Rechtsgrundlage. Gleiches gilt für eine Einwilligung der betroffenen Person: Trotz Einwilligung bedarf es einer gesetzlichen Grundlage.
● In der gesetzlichen Grundlage müssen zumindest Ziele der Verarbeitung, die zu verarbeitenden personenbezogenen Daten und die Zwecke der Verarbeitung festgelegt sein.
● Die Weiterverwendung für andere kompatible Zwecke unter erleichterten Voraussetzungen (ohne neue Rechtsgrundlage) ist nicht zulässig.
● Die DSRL-PJ erlaubt wie bereits erwähnt gewisse Einschränkungen des Auskunftsrechts der betroffenen Person[26] sowie bei den Informationspflichten des Verantwortlichen[27].

1.3. DSG

Die DSRL-PJ wurde in der österreichischen Rechtsordnung durch das 3. Hauptstück des DSG umgesetzt. Dieses 3. Hauptstück geht gem § 4 Abs 1 letzter HS DSG der DSGVO und auch den übrigen Bestimmungen des DSG vor.[28] Die Bestimmungen des 3. Hauptstücks des DSG gelten für die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung.[29]

Darüber hinaus normiert § 1 Abs 1 DSG das Grundrecht auf Datenschutz[30], wonach jedermann im Hinblick auf die Achtung seines Privat- und Familienlebens Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat, soweit ein schutzwürdiges Interesse daran besteht.

1.4. StPO

Für die Verarbeitung personenbezogener Daten in Strafverfahren finden die Bestimmungen der StPO Anwendung.[31] Die StPO enthält in §§ 74 f leg cit Bestimmungen über die Verarbeitung von (personenbezogenen) Daten. Gem § 74 Abs 1 1. Satz StPO dürfen Kriminalpolizei, Staatsanwaltschaft und Gericht im Rahmen ihrer Aufgaben die *hierfür erforderlichen* personenbezogenen Daten verarbeiten. Kriminalpolizei, Staatsanwaltschaft und Gericht haben beim Verarbeiten personenbezogener Daten den Grundsatz der Gesetz- und Verhältnismäßigkeit (§ 5 StPO) zu beachten. Jedenfalls haben sie schutzwürdige Interessen der betroffenen Personen an der Geheimhaltung zu wahren und vertraulicher Behandlung personenbezogener Daten Vorrang einzuräumen. Bei der Verarbeitung besonderer Kategorien[32] und strafrechtlich relevanter personenbezogener Daten haben sie angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der betroffenen Personen zu treffen.[33] § 74 Abs 1 2. Satz StPO verweist auf die Anwendbarkeit des DSG, soweit in der StPO nichts anderes bestimmt wird. Die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen – wie in

[24] Art 8 Abs 1 DSRL-PJ.
[25] Vgl Art 6 Abs 1 lit f DSGVO.
[26] Art 15 DSRL-PJ.
[27] Art 13 Abs 3 DSRL-PJ.
[28] *Heißl* in *Knyrim,* DatKomm, Art 2 Rz 82 (Stand Februar 2019).
[29] § 36 Abs 1 DSG.
[30] Dieses findet auch im Strafverfahren anhängig, auch wenn es nicht im 3. Hauptstück des DSG normiert ist.
[31] § 85a Abs 1 GOG.
[32] § 39 DSG.
[33] § 74 Abs 2 StPO.

concreto §§ 74 f StPO – gehen als leges speciales den allgemeinen Regelungen des 3. Hauptstücks des DSG vor.[34]

1.5. GOG, StAG

Ebenso finden sich datenschutzrechtlich relevante Bestimmungen im GOG[35] sowie StAG[36] wieder. Aufgrund des geringen Anwendungsbereichs dieser Bestimmungen wird auf diese nicht gesondert eingegangen.

2. Grundsätze für die Datenverarbeitung im Strafverfahren

2.1. Allgemeines

Die einzuhaltenden Grundsätze für eine Datenverarbeitung im Strafverfahren sind nur in geringem Ausmaß unterschiedlich zu den allgemeinen Grundsätzen der DSGVO. Personenbezogene Daten, welche in einem Strafverfahren verarbeitet werden,

- müssen auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden[37],
- müssen für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden[38],
- müssen dem Verarbeitungszweck entsprechen und müssen maßgeblich sein und dürfen in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein[39],
- müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden[40],
- dürfen nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht[41],
- müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.[42]

Diese Grundsätze der Datenverarbeitung finden sich auch in § 74 StPO – teilweise direkt und teilweise indirekt – wieder. § 74 Abs 1 1. Satz StPO legt fest, dass nur die im Rahmen der Aufgaben erforderlichen personenbezogene Daten verarbeitet werden dürfen. Auch die Einhaltung der Gesetz- und

---

[34] AB 1761 BlgNR 25. GP 18.
[35] Gesetz vom 27.11.1896, womit Vorschriften über die Besetzung, innere Einrichtung und Geschäftsordnung der Gerichte erlassen werden (Gerichtsorganisationsgesetz – GOG), StF: RGBl 1896/217 idgF.
[36] Bundesgesetz vom 5.3.1986 über die staatsanwaltschaftlichen Behörden (Staatsanwaltschaftsgesetz – StAG), StF: BGBl 1986/164 idgF.
[37] § 37 Abs 1 Z 1 DSG; Art 4 Abs 1 lit a RSRL-PJ.
[38] § 37 Abs 1 Z 2 DSG; Art 4 Abs 1 lit b DSRL-PJ.
[39] § 37 Abs 1 Z 3 DSG; Art 4 Abs 1 lit c DSRL-PJ.
[40] § 37 Abs 1 Z 4 DSG, Art 4 Abs 1 lit d DSRL-PJ.
[41] § 37 Abs 1 Z 5 DSG, Art 4 Abs 1 lit e DSRL-PJ.
[42] § 37 Abs 1 Z 6 DSG; Art 4 Abs 1 lit f DSRL-PJ.

Verhältnismäßigkeit ist ausdrücklich normiert.[43] Es besteht daher eine Geheimhaltungs(wahrungs)pflicht sowie eine Vertraulichkeitsverpflichtung auch nach der StPO.[44] Durch den Verweis in § 74 Abs 1 2. Satz StPO sind jedoch auch die weiteren oben dargestellten Grundsätze der Datenverarbeitung einzuhalten.

2.2. In concreto: Kriterien für die Verarbeitung personenbezogener Daten im Strafakt

Die Grundsätze der Datenverarbeitung sind freilich auch für die Frage, ob bzw welche personenbezogene Daten in einen Strafakt aufgenommen (ergo verarbeitet) werden dürfen, relevant. Wie bereits festgehalten, dürfen personenbezogene Daten nicht in einer mit dem eindeutigen und rechtmäßigen Zweck nicht vereinbarenden Weise verarbeitet werden.[45] Ebenso müssen personenbezogene Daten dem Verarbeitungszweck entsprechen, müssen maßgeblich sein und dürfen in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein.[46] § 34a Abs 2 1. Satz StAG hält ebenfalls fest, dass in die Ermittlungsakten, Register, Geschäftsbehelfe sowie Tagebücher nur solche Daten aufgenommen werden, die *erforderlich* sind, um den Zweck des Registers, Geschäftsbehelfs, Tagebuchs oder Ermittlungsakts zu erfüllen.

Bei der Datenverarbeitung – samt der Aufnahme und Verarbeitung personenbezogener Daten im Ermittlungsakt – haben die Strafverfolgungsbehörden daher den Verhältnismäßigkeitsgrundsatz zu wahren. Dies ist sowohl durch § 74 Abs 2 iVm § 5 StPO als auch durch § 37 Abs 1 Z 2 und 3 DSG und § 34a Abs 2 StAG normiert.[47] Orientiert an den dargelegten Grundsätzen der Datenverarbeitung ist daher bei jeder Datenerhebung und -verarbeitung im Strafverfahren auch die Verhältnismäßigkeitsprüfung nach § 5 StPO vorzunehmen.[48] Es ist sohin beispielsweise unzulässig, wenn seitens der Strafverfolgungsbehörden mehr personenbezogene Daten – vor allem auch in Ermittlungsakten, Register und Tagebücher – verarbeitet werden als zwingend erforderlich. Die Strafverfolgungsbehörden müssen sich dabei jedenfalls die Frage stellen: Ist die Verarbeitung bestimmter personenbezogener Daten zu legitimen Zwecken – insbesondere zur Strafverfolgung – tatsächlich erforderlich und – vor allem in Hinblick auf das verfassungsrechtlich gewährleistete Grundrecht auf Datenschutz – verhältnismäßig?

3. Rechte des Betroffenen im Strafverfahren

Auch im Strafverfahren haben betroffene Personen datenschutzrechtliche Rechte (neben dem allgemeinen Grundrecht auf Datenschutz gem § 1 Abs 1 DSG). Im 3. Hauptstück des DSG sind einige Rechte betroffener Personen normiert (Recht auf Information, Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung). Bereits das DSG schränkt diese Rechte ein. So ist das Recht auf Information und Auskunft beschränkt, soweit dies im Einzelfall unbedingt erforderlich und verhältnismäßig ist,

● um zu gewährleisten, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, insbesondere durch die Behinderung

---

[43] § 74 Abs 2 1. Satz StPO.
[44] § 74 Abs 2 StPO.
[45] § 37 Abs 1 Z 2 DSG; Art 4 Abs 1 lit b DSRL-PJ.
[46] § 37 Abs 1 Z 3 DSG; Art 4 Abs 1 lit c DSRL-PJ.
[47] Ebenso auch durch den (jedoch nicht unmittelbar anwendbaren) Art 4 Abs 1 lit b und c DSRL-PJ.
[48] *Reindl-Krauskopf* in WK StPO § 74 Rz 28 (Stand 1.4.2011, rdb.at).

behördlicher oder gerichtlicher Untersuchungen, Ermittlungen oder Verfahren,
- zum Schutz der öffentlichen Sicherheit,
- zum Schutz der nationalen Sicherheit,
- zum Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich,
- zum Schutz der militärischen Eigensicherung oder
- zum Schutz der Rechte und Freiheiten anderer. [49]

Im Strafverfahren nach der StPO finden die im DSG explizit normierten Rechte nur eingeschränkt Anwendung. Begründet wird dies damit, dass die einschlägigen Regelungen der StPO zu bestimmten Datenverarbeitungen als leges speciales den allgemeinen Regelungen des 3. Hauptstücks des DSG vorgehen. Die Regelungen der StPO über Akteneinsicht oder Verständigungspflichten sind daher als leges speciales zum 3. Hauptstück des DSG zu betrachten. Informationsverpflichtungen sind etwa in § 50, § 138 Abs 5, § 139 Abs 2 StPO geregelt, wobei diese im Einklang mit der für das Strafverfahren wesensimmanenten Zielsetzung der Aufklärung von Straftaten und Verfolgung verdächtiger Personen unter Wahrung der Rechte Verdächtiger bzw Beschuldigter auch dem Umstand einer möglichen Gefährdung des Zwecks des strafrechtlichen Ermittlungsverfahrens Rechnung tragen. Die Auskunft innerhalb der StPO wird typischerweise über die Regelung der Akteneinsicht präzisiert. Daneben bleibe kein Raum für das Auskunftsrecht nach dem DSG.[50] Das Auskunftsrecht iSd § 44 DSG darf und kann daher auch nicht zur Umgehung des in der StPO geregelten, speziellen Einsichtsrechts (va Akteneinsicht) herangezogen werden.[51]

Das Berichtigen und Löschen personenbezogener Daten wird in § 75 StPO geregelt. Wo es an entsprechenden Regelungen in der StPO fehlt, finden gem § 74 Abs 1 StPO die Bestimmungen des DSG subsidiär im Strafverfahren Anwendung.

Wenngleich sich die Rechte des Betroffenen im Strafprozess sohin weitestgehend nach der StPO richten, sei nochmals festgehalten, dass dennoch jegliche Verarbeitung personenbezogener Daten auch im Anwendungsbereich der StPO den unter Pkt 3 dargelegten Grundsätzen der Datenverarbeitung – vor allem auch der Wahrung des Grundrechts auf Datenschutzes unter Einhaltung der Verhältnismäßigkeit – zu entsprechen hat.

4. Durchsetzung von Betroffenenrechten im Strafverfahren

4.1. Allgemeines

Anders als die Frage, ob und inwieweit personenbezogene Daten von den Strafverfolgungsbehörden überhaupt verarbeitet werden dürfen, wurde der Rechtsschutz gegen Fehlverhalten der Strafverfolgungsbehörden nicht verändert.[52] Schon nach der alten Rechtslage waren qua Verweis in § 74 Abs 1 StPO idF BGBl I 2004/19 sämtliche Datenschutzrechte des DSG 2000 Teil der StPO, soweit die StPO keine spezielleren Bestimmungen vorgesehen hat. Soweit also die StPO direkt oder subsidiär das DSG 2000 ein subjektives Recht einer betroffenen Person auf Auskunft, Löschung, Geheimhaltung oä beinhaltet hat, war dies gleichzeitig ein subjektives Recht iSd § 106 Abs 1 StPO und konnte mittels

[49] § 43 Abs 4, § 44 Abs 2 DSG.
[50] AB 1761 BlgNR 25. GP 23; ErläutRV 65 BlgNR 26. GP 153; *Reindl-Krauskopf* in WK StPO § 74 Rz 60 (Stand 1.4.2011, rdb.at).
[51] Zum Spezialfall der Akteneinsicht bei der Kriminalpolizei siehe noch unten.
[52] Lediglich im subsidiären Rechtsschutzregime des GOG kam es zu Änderungen, siehe hierzu 4.2..

Einspruchs wegen Rechtsverletzung und/oder Beschwerde auch durchgesetzt werden.[53] Einzig für Datenschutzverletzungen durch die Kriminalpolizei musste, soweit die Datenverarbeitung aus Eigenem erfolgt ist, die Datenschutzkommission[54] angerufen werden[55], nachdem der VfGH § 106 Abs 1 Satz 1 StPO als verfassungswidrig aufgehoben hatte.[56]

An diesen Grundprinzipien hat sich auch durch BGBl I 2018/32 nichts geändert. Zu einem gewissen Grad bleibt somit nach wie vor das datenschutzrechtliche Regime über die Durchsetzung von Betroffenenrechten in die StPO eingegliedert. So hat jede betroffene Person, deren personenbezogene Daten von Strafverfolgungsbehörden verarbeitet werden, gegenüber dem Verantwortlichen insbesondere ein Recht auf Auskunft, Berichtigung und allenfalls auch Löschung seiner Daten, das mit den Mitteln der StPO durchgesetzt werden kann.[57] Das erfolgversprechendste Mittel zum Zweck ist daher auch vom jeweiligen Verfahrensstadium abhängig: Im Ermittlungsverfahren sind auch Datenschutzverletzungen per Einspruch wegen Rechtsverletzung geltend zu machen, soweit diese nicht durch einen Gerichtsbeschluss erfolgt sind. Mit dem Übergang in das Hauptverfahren sind Datenschutzrechte primär gegenüber diesem – mittels entsprechenden Antrags und allenfalls Beschwerde gegen einen abweisenden Beschluss – geltend zu machen. Gem § 210 Abs 2 StPO wird das Gericht durch Anklageerhebung Leiter des Verfahrens, womit auch die datenschutzrechtliche Verantwortlichkeit übergeht. Ein Einspruch wegen Rechtsverletzung bleibt nach allgemeinen Regeln zulässig[58] und ist insbesondere dann tunlich, wenn die Erfassung von Daten oder die Verletzung der Geheimhaltungspflicht durch die Staatsanwaltschaft gerügt werden soll. Effektive Rechtsdurchsetzung, insbesondere durch Löschung, kann in diesem Stadium aber nur noch vor dem HV-Gericht erfolgen. Für datenschutzrechtliche *Auskunftsrechte* ergibt sich aus der Verzahnung zwischen StPO und DSG sogar die teilweise Schließung einer bestehenden Rechtsschutzlücke: Die StPO beinhaltet mit den Bestimmungen über die Akteneinsicht für Beschuldigte, Opfer und Privatbeteiligte, Privat- und Subsidiarankläger sowie für alle anderen Personen mit einem rechtlichen Interesse (§ 77 StPO) detaillierte Regelungen zur Auskunft (auch) über eigene personenbezogene Daten und geht somit gem § 74 Abs 1 StPO dem eigentlichen Datenschutzrecht vor. Für nicht verfahrensbeteiligte Personen ergibt sich aus dem datenschutzrechtlichen Auskunftsrecht ein begründetes rechtliches Interesse iSd § 77 Abs 1 StPO. Wird ein Antrag auf Akteneinsicht nicht erfüllt, steht Beschwerde und Einspruch wegen Rechtsverletzung offen. Da die StPO keinen Rechtsschutz gegen eine Verweigerung der Akteneinsicht durch die Kriminalpolizei vorsieht und diese als schlichtes kriminalpolizeiliches Handeln auch nicht vor dem Verwaltungsgericht bekämpft werden kann, wird häufig geäußert, dass eine solche Verweigerung nicht bekämpfbar ist.[59] Dies ist insoweit wohl unrichtig, als Einsicht in personenbezogene Daten begehrt wird, die den Antragsteller betreffen. Es spricht nichts dagegen, für diese Fälle – wie generell für verwaltungsbehördliche Verletzungen des datenschutzrechtlichen Auskunftsrechts – eine Beschwerde an die Datenschutzbehörde zuzulassen, zumal die StPO diesen Fall eben nicht im Sinn des § 74 Abs 1 selbst regelt. Die Kriminalpolizei müsste den Antragsteller über dieses Recht sogar informieren (§ 44 Abs 3 DSG). In der Praxis erfolgt dies – soweit ersichtlich – bislang nicht. Die Durchsetzung von Berichtigungen und Löschungen verläuft weitestgehend kongruent. Einzig bei Registern lassen sich Berichtigungen nämlich

[53] *Reindl-Krauskopf* in WK StPO § 74 Rz 63 (Stand 1.4.2011, rdb.at).
[54] Nunmehr: Datenschutzbehörde.
[55] *Reindl-Krauskopf* in WK StPO § 74 Rz 65 (Stand 1.4.2011, rdb.at).
[56] VfGH 16.12.2010, G 259/09 ua sowie nochmals VfGH 30.6.2015, VfSlg 19.991.
[57] *Reindl-Krauskopf*, Durchsetzung der Datenschutzrechte bei Akten der Strafgerichtsbarkeit, altes und neues Recht, JBl 2019, 737.
[58] *Birklbauer* in WK StPO § 210 Rz 21 f (Stand 20.12.2018, rdb.at).
[59] Anstatt vieler: *Hinterhofer/Oshidari*, System des österreichischen Strafverfahrens 7.1078.

tatsächlich durchführen. Alle übrigen Datenverarbeitungen durch die Ermittlungsbehörden sind, aufgrund der nach wie vor nicht digitalisiert geführten Akten, nur durch Löschung der unrichtigen und Neuerfassung der richtigen personenbezogenen Daten umsetzbar.

Einen darauf gerichteten Antrag kann jeder Betroffene – auch nach Ende des Verfahrens[60] – bei der Staatsanwaltschaft oder beim Gericht einbringen. Das Gericht hat einen solchen Antrag mit Beschluss zu erledigen, Staatsanwaltschaften dem Antragsteller unverzüglich mitzuteilen, ob dem Antrag nachgekommen wird. Wird dem Antrag nicht nachgekommen, steht dem Betroffenen der strafprozessuale Zug ans Landes- bzw Oberlandesgericht zu.

Fraglich ist, ob es im Ermittlungsverfahren vor Erheben eines Einspruchs wegen Rechtsverletzung wegen unterbliebener Löschung oder Berichtigung eines entsprechenden Antrags bedarf. UE ist ein solcher Antrag – wenngleich aus Effizienzgründen ratsam – nicht erforderlich. Denn Voraussetzung insbesondere des Rechts auf Löschung ist es, dass Daten widerrechtlich verarbeitet, insbesondere gespeichert werden. Die widerrechtliche Speicherung liegt einerseits im Zeitpunkt des Löschungsantrags bereits vor, andererseits beruht sie in aller Regel auf einer bereits rechtswidrigen Datenerfassung.[61] Bereits durch die widerrechtliche Speicherung wird die betroffene Person in ihrem subjektiven (Grund-) Recht auf Datenschutz gem § 1 Abs 1 DSG verletzt.[62] Ein rechtswidrig von der Staatsanwaltschaft nicht erfüllter Löschungsantrag wäre somit nur noch eine weitere Rechtsverletzung, die mit Einspruch aufgegriffen werden könnte. Er ist aber dann für effektiven Rechtsschutz erforderlich, wenn die 6-Wochen-Frist des § 106 Abs 3 StPO seit Bekanntwerden der rechtswidrigen Datenverarbeitung abgelaufen ist: Da ein rechtswidrig nicht erfüllter Löschungsantrag eine eigene Rechtsverletzung ist, löst die Ablehnung bzw Untätigkeit der Staatsanwaltschaft eine neue Frist aus.

4.2. Rechtsschutz nach GOG

Ein subsidiärer Rechtsschutz bei Datenschutzverletzungen ist in §§ 85, 85a GOG (für Angelegenheiten der Strafgerichtsbarkeit) sowie in § 34a Abs 2a StAG[63] (für Angelegenheiten der Staatsanwaltschaften) normiert. Diese Bestimmungen kommen aufgrund ihrer Ausgestaltung als subsidiärer Rechtsschutz nur dort zum Tragen, wo die StPO für die Durchsetzung der Datenschutzrechte keine ausreichenden Instrumente vorsieht.[64] Der Anwendungsbereich der Bestimmung ist im Strafverfahren denkbar klein, weil typischerweise nach der StPO mit Einspruch wegen Rechtsverletzung, Beschwerde oder Nichtigkeitsbeschwerde/Berufung gegen das Urteil vorgegangen werden kann, um Datenschutzverletzungen geltend zu machen. Erst wo diese Möglichkeiten enden, ist das GOG einschlägig.[65] Diese Bestimmungen dienen (etwa im Bereich der Geschäftsregister) aber dazu, dort Lücken im Rechtsschutz zu schließen, wo die Verfahrensordnung einen solchen nicht bietet.[66]

5. Praktische Handhabung

Das strafprozessuale Datenschutzregime kann ansehnlich anhand eines Zufallsfunds-Beispiels

[60] OGH 2.4.2019, 11 Os 69/18h.
[61] Vgl § 45 Abs 2 Z 3 DSG.
[62] Vgl *Chausse/Kudrna*, Strafrechtliche Folgen eines Missbrauchs des Auskunftsrechts (Teil 1), Dako 2019/57.
[63] Welcher wiederum auf das GOG verweist.
[64] OGH 2.4.2019, 11 Os 69/18h; siehe auch *Reindl-Krauskopf*, JBl 2019, 737.
[65] ErläutRV 65 BlgNR 26. GP 154; *Reindl-Krauskopf* in WK StPO § 74 Rz 67 (Stand 1.4.2011, rdb.at).
[66] ErläutRV 65 BlgNR 26. GP 154.

zusammengefasst werden:

Die Kriminalpolizei findet im Zuge einer Hausdurchsuchung wegen eines Untreue-Verdachts im Rahmen der beruflichen Tätigkeit des Beschuldigten auch diverse Schreiben der Ex-Frau des Beschuldigten, in denen sich diese über zu geringe Unterhaltszahlungen durch den Beschuldigten beschwert. Die Kriminalpolizei stellt die Schreiben sicher und legt diese gemeinsam mit einem kurzen Bericht an die zuständige Staatsanwaltschaft vor. Die Unterlagen stehen in keinem Zusammenhang zum bisherigen Verfahren. Die Staatsanwaltschaft nimmt sie dennoch zum selben Akt.

Hausdurchsuchung, Sicherstellung sowie die Behandlung von Zufallsfunden sind in der StPO geregelt. Es besteht somit eine generelle Rechtsgrundlage für die Verarbeitung von Ergebnissen. Diese besteht insoweit, als die Verarbeitung für den Zweck des Ermittlungsverfahrens – nämlich Straftaten aufzuklären und zu verfolgen – erforderlich ist. In anderen Worten: Die verarbeiteten Daten müssen erforderlich sein, um einen strafrechtlich relevanten Sachverhalt aufzuklären.

Insoweit wird es vertretbar sein, diese – den privaten Lebensbereich des Beschuldigten und seiner Familie betreffenden – Daten zu verarbeiten. Diese Begründung ist aber nur insoweit belastbar, als sich aus den Schreiben klar ergibt, dass der Beschuldigte Unterhaltszahlungen nur unterhalb seiner Unterhaltspflicht (und nicht bloß nach dem subjektiven Empfinden der Ex-Frau zu gering) leistet sowie dass zumindest ein Anfangsverdacht hinsichtlich der übrigen Tatbestandsmerkmale des § 198 StGB denkbar ist.

Soweit die Verarbeitung an sich rechtmäßig ist, ist sie auch daran zu messen, ob § 74 Abs 2 StPO – der möglichst schonenden, vertraulichen Verarbeitung – hinreichend Rechnung getragen wird. Grundsätzlich ist die Vorgehensweise der Staatsanwaltschaft, die Unterlagen zum bisherigen Akt zu nehmen, im Einklang mit § 26 Abs 1 StPO. UE hat hier aber – vor allem, wenn im "Stammakt" mehrere Beteiligte akteneinsichtsberechtigt sind – der Datenschutz iS des § 74 Abs 2 StPO dahingehend Vorrang, dass die Staatsanwaltschaft von ihrer Möglichkeit, den neuen Tatverdacht gem § 27 StPO abzutrennen und gesondert zu ermitteln, zwingend Gebrauch machen muss. Tut sie dies nicht, verletzt sie den Beschuldigten uE in seinem Recht auf Datenschutz, was dieser mit Einspruch wegen Rechtsverletzung erfolgversprechend geltend machen könnte.

6. Fazit

Wenngleich praktisch oft wenig beachtet, bestehen auch im Strafprozess weitreichende Datenschutzrechte. Diese richten sich nicht primär nach der DSGVO, sondern nach StPO, DSG und DSRL-PJ. Insbesondere haben Betroffene (neben dem allgemein bekannten Recht auf Akteneinsicht sowie den prozessualen Informationsrechten) auch ein Recht auf Berichtigung und allenfalls Löschung rechtswidrig verarbeiteter oder unrichtiger Daten.

Im Sinne eines effektiven Datenschutzes obliegt es den Strafverfolgungsbehörden, von ihren prozessualen Möglichkeiten iS des § 74 Abs 2 StPO so Gebrauch zu machen, dass dem Datenschutzinteresse des Betroffenen bestmöglich Rechnung getragen wird. Neben der bekannten Thematik der Beschränkung der Akteneinsicht Verfahrensbeteiligter[67] bedeutet dies insbesondere auch, dass von der Möglichkeit von Verfahrenstrennungen gem § 27 StPO Gebrauch zu machen ist, soweit in Verfahren mit mehreren Beschuldigten einzelne Fakten nur einen Beschuldigten betreffen und die Aufarbeitung

[67] OGH 23.8.2017, 15 Os 7/17v.

dieses Faktums unter der Akteneinsicht der übrigen Beschuldigten jenen unverhältnismäßig in seinen Geheimhaltungsinteressen beeinträchtigen würde.

Für den Verlag:

Alexander Stücklberger

stuecklberger@btp.at

Georg Kudrna

Georg.kudrna@rwk.at