# I. Einleitung

## A. Datenschutz im Strafprozess: Warum?

Durch die Ausbreitung der **elektronischen Datenverarbeitung** in sämtliche Lebensbereiche können seit den 1960er-Jahren massenhaft Informationen über Personen gesammelt, gespeichert, übermittelt, mit anderen Informationen verknüpft und ausgewertet werden.[1] Damit verbunden sind bedeutende **soziale und wirtschaftliche Entwicklungen** wie das Aufkommen des Internets und eines umfassenden Datenhandels.[2] Auch für die **Strafverfolgung** eröffnen sich neue technische Möglichkeiten. So erlaubt die elektronische Datenverarbeitung die Ansammlung großer Datenbestände, die in der Folge systematisch durchsucht, ohne großen technischen Aufwand zwischen unterschiedlichen Behörden und Aufgabenbereichen transferiert und damit auch für die Strafverfolgung nutzbar gemacht werden können.

Allerdings führt diese Effizienz der Datenverarbeitung auch zu **beträchtlichen Gefahren für den Einzelnen.** Durch die technisch unbegrenzte und für den Einzelnen nicht überblickbare Speicherung von Daten lässt sich ein umfassendes Bild des Betroffenen zeichnen, dass seine politischen, religiösen und sonstigen persönlichen Anschauungen sowie seine sozialen Beziehungen offenlegt und damit eine **umfassende Kontrolle** des Betroffenen ermöglicht.[3] Insofern kann der ungeregelte Umgang mit personenbezogenen Daten letztlich die **selbstbestimmte Gestaltung des Lebens** bedrohen.[4]

In besonderer Weise gilt das für **Datenverarbeitungen durch Strafverfolgungsbehörden.** Diese klären die Verletzungen elementarer Regeln des gesellschaftlichen Zusammenlebens auf und sind deswegen mit weitreichenden Eingriffsbefugnissen

---

1 Vgl *Berka*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, in *ÖJT* (Hrsg), 18. ÖJT Band I/1 (27 ff); *Tichy/Peissl*, Beeinträchtigung der Privatsphäre in der Informationsgesellschaft, in *ÖJK* (Hrsg), Grundrechte in der Informationsgesellschaft (2001) 22 (24 ff); *Souhrada-Kirchmayer*, Zur Geschichte des europäischen Datenschutzrechts, in FS Ogris (2010) 499 (499 f); *Wiederin*, Privatsphäre und Überwachungsstaat (2003) 13 f; *Eberhard* in *Korinek/Holoubek* ua, Bundesverfassungsrecht § 1 DSG Rz 1. Zum Begriff der elektronischen (automatisierten) Verarbeitung vgl *Heißl* in *Knyrim*, DatKomm Art 2 DSGVO Rz 48; *Ernst* in *Paal/Pauly*, DS-GVO BDSG[3] Art 2 Rz 5 f; *Zerdick* in *Ehmann/Selmayr*, Datenschutz-Grundverordnung[2] Art 2 Rz 3.

2 *Lachmayer*, Datenschutzrecht als Öffentliches Wirtschaftsrecht, in *Jahnel* (Hrsg), Jahrbuch Datenschutzrecht und E-Government 2013 (2013) 9 (16 ff); *Eberhard* in *Korinek/Holoubek* ua, Bundesverfassungsrecht § 1 DSG Rz 2; *Berka*, 18. ÖJT Band I/1, 10 f.

3 Vgl *Wiederin*, Überwachungsstaat 14; *Berka/Binder/Kneihs*, Die Grundrechte[2] (2019) 388 f; *Tichy/Peissl* in *ÖJK*, Grundrechte 22 (insb 31 ff); *Slobogin*, Privacy at Risk (2007) 3 ff; vgl auch ErwG 3 JI-RL, ErwG 6 DSGVO; grundlegend zu alldem BVerfG 15. 12. 1983, 1 BvR 209/83 Rz 145.

4 *Ennöckl*, Der grundrechtliche Schutz der Privatsphäre (2014) 212; *Wiederin*, Überwachungsstaat 14; BVerfG 15. 12. 1983, 1 BvR 209/83 Rz 146.

ausgestattet, die es in dieser Form in keinem anderen Bereich gibt. Das betrifft erstens die **Art des Zugriffs** auf Daten, da Datenverarbeitungen hier oft mit dem Einsatz von Zwangsgewalt verbunden sind bzw im Geheimen stattfinden, wodurch die Daten der Kontrolle durch den Betroffenen gänzlich entzogen sind.[5] Zweitens zeichnen sich strafbehördliche Datenverarbeitungen durch die **Art der verarbeiteten Daten** aus: Die StPO ermächtigt zur Verarbeitung von Daten zum Gesundheitszustand, zum Sexualleben sowie zu anderen höchstpersönlichen Bereichen und macht damit auch vor der Intimsphäre des Betroffenen nicht Halt.[6]

Diesen Risiken der elektronischen Datenverarbeitung soll das **Datenschutzrecht** begegnen.[7] In Österreich hat der Gesetzgeber vergleichsweise früh reagiert und 1978 das **Datenschutzgesetz** erlassen, das in **§ 1** ein „Grundrecht auf Datenschutz" enthält.[8] Parallel dazu hat der EGMR seine Rsp zu **Art 8 EMRK** weiterentwickelt und beurteilt Datenverarbeitungen seitdem als möglichen Eingriff in den Schutzbereich.[9] Die dabei aufgestellten Grundsätze zu Datenverarbeitungen im Strafprozess finden regelmäßig auch Eingang in Entscheidungen von EuGH und VfGH, etwa im Zusammenhang mit geheimen Überwachungsmaßnahmen, der Verarbeitung genetischer Daten und der Sicherstellung von Datenträgern.[10] In jüngerer Zeit ist die Weiterentwicklung des Datenschutzrechts vor allem mit Impulsen auf europäischer Ebene verbunden, insb durch den Schutz personenbezogener Daten nach **Art 8 GRC,** die Datenschutz-RL Justiz/Inneres **(JI-RL)**[11] und die im Strafverfahren grundsätzlich nicht anwendbare Datenschutzgrundverordnung **(DSGVO)**[12].

Auf allen angesprochenen Ebenen soll das Datenschutzrecht die **freie Entfaltung der Persönlichkeit** vor einer informationellen Übermacht staatlicher und privater

5 Zur Schwierigkeit eines effektiven Rechtsschutzes bei geheimen Maßnahmen vgl *Merli*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit – Die europäische Dimension, in *ÖJT* (Hrsg), 18. ÖJT Band I/2 (2012) 55 (74 f); *Zerbes*, Spitzeln, Spähen, Spionieren (2010) 107 ff; *Berka*, 18. ÖJT Band I/1, 122 ff; *Ennöckl*, Privatsphäre 299 ff.

6 Datenschutzrechtlich geht es dabei um sogenannte „besondere Kategorien personenbezogener Daten", die nur nach den strengen Grundsätzen des Art 10 JI-RL verarbeitet werden dürfen.

7 *Souhrada-Kirchmayer* in FS Ogris 499; *Berka/Binder/Kneihs,* Grundrechte[2] 389; *Berka*, 18. ÖJT Band I/1, 27 ff; *Tichy/Peissl* in *ÖJK*, Grundrechte 22 (39).

8 Datenschutzgesetz BGBl 1978/565; dazu ausführlich EBRV 72 BlgNR 14. GP 8. Vgl auch *Souhrada-Kirchmayer* in FS Ogris 499; *Knyrim*, Entwicklung und Struktur des Datenschutzrechts, in *Knyrim* (Hrsg), Datenschutzrecht[4] (2020) Rz 2.1 ff; *Berka*, 18. ÖJT Band I/1, 30 ff; *Eberhard* in *Korinek/Holoubek* ua, Bundesverfassungsrecht § 1 DSG Rz 1 ff.

9 *Klaushofer/Kneihs* in *Kneihs/Lienbacher*, Rill-Schäffer-Kommentar Art 8 MRK Rz 28; *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention[7] (2021) § 22 Rz 10 mN; vgl dazu noch ausführlich im grundrechtlichen Teil S 27 ff.

10 Zum Einfluss der EGMR-Rsp zu Art 8 EMRK vgl *Grabenwarter,* Das Recht auf informationelle Selbstbestimmung im Europarecht und im Verfassungsrecht, AnwBl 2015, 404; zur Sicherstellung von Datenträgern jüngst VfGH 14. 12. 2023, G352/2021.

11 Richtlinie (EU) 2016/680.

12 Verordnung (EU) 2016/679.

Akteure schützen und dient damit dem **Persönlichkeitsschutz.**[13] In Abgrenzung zu anderen, schon deutlich länger bestehenden Teilaspekten des Persönlichkeitsschutzes[14] bezieht sich das Datenschutzrecht dabei nicht auf ausgewählte Bereiche der „realen Außenwelt", sondern knüpft an die **„Repräsentation des Menschen"** in einer technisch definierten Form – **als Datum** – an.[15] Somit verfolgt das Grundrecht auf Datenschutz einen stark technisch geprägten Ansatz.

Das Datenschutzrecht ist allerdings nicht bei diesem Schutz der Persönlichkeit vor den Gefahren der elektronischen Verarbeitung stehengeblieben, sondern geht heute **in zweifacher Hinsicht darüber hinaus.** Zum einen erfassen die meisten datenschutzrechtlichen Vorschriften neben der elektronischen Datenverarbeitung zumindest auch einzelne Formen der **manuellen Verarbeitung.**[16] Zum anderen werden nicht nur Daten mit einem unmittelbaren Bezug zur Persönlichkeit geschützt, sondern teilweise auch **Daten juristischer Personen.**[17] Dadurch kam es zu einer partiellen **Entkopplung vom eigentlichen Schutzanliegen.**[18]

## B. Datenschutz- und Strafverfolgungsinteressen im Verhältnis

### 1. Datenschutz als Hindernis effektiver Strafverfolgung

Das Datenschutzrecht räumt dem Betroffenen eine **Sphäre der Geheimhaltung** ein, über die er autonom verfügen und daher vor Zugriffen anderer abschirmen kann. Damit steht das Datenschutzrecht tendenziell in einem **Spannungsverhältnis** zur Strafverfolgung, die bei der Aufklärung von Verdachtsmomenten auf die Verarbeitung personenbezogener Daten – etwa den Zugriff auf die private Kommunikati-

13 Vgl *Berka*, 18. ÖJT Band I/1, 59, 83 ff, 148; *Schauer* in *Kletečka/Schauer*, ABGB-ON[1.02] § 16 Rz 11; *Ennöckl*, Privatsphäre 171; *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 2/42; *Grabenwarter/Pabel*, EMRK[7] § 22 Rz 11.

14 Zur Begründung des Privatsphärenschutzes vgl insb *Warren/Brandeis*, The Right to Privacy, Harvard Law Review 1890, 193 sowie die historischen Überblicke bei *Richardson*, Law and the Philosophy of Privacy (2016); *Slobogin*, Privacy at Risk (2007) 21 ff; *Wiederin*, Der grundrechtliche Schutz der Privatsphäre: Eine Entwicklungsgeschichte, in *Peissl* (Hrsg), Privacy (2003) 31; *Kienapfel*, Privatsphäre und Strafrecht (1969) 14 ff; *Bennett*, Information Privacy and „Datenschutz": Global Assumptions and International Governance, in *Peissl* (Hrsg), Privacy 69.

15 *Ennöckl*, Privatsphäre 212 f, vgl auch 125 (Fn 646) ebenda. Zur historischen Verknüpfung des Datenschutzrechts mit dem Schutz der Privatsphäre vgl auch die Nachweise in Fn 149.

16 Bspw unterscheidet § 1 Abs 1 DSG generell nicht zwischen der automatisierten und der manuellen Verarbeitung (vgl dazu ausführlich im grundrechtlichen Teil S 19 f). Die JI-RL bezieht sich neben der ganz oder teilweise automatisierten (elektronischen) Verarbeitung auch auf die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert werden (Art 2 Abs 2 JI-RL); ähnlich auch die Nebenrechte auf Auskunft, Richtigstellung und Löschung nach § 1 Abs 3 DSG.

17 Zu § 1 DSG vgl VfSlg 19.702/2012; *Spitzbart*, Grundrecht auf Datenschutz für juristische Personen (2014) 17 f; *Wiederin*, Schutz der Privatsphäre, in *Merten/Papier/Kucsko-Stadlmayer* (Hrsg), Handbuch der Grundrechte in Deutschland und Europa, Band VII/1[2] (2014) 363 (367).

18 *Berka*, 18. ÖJT Band I/1, 63 f.

on sowie den Abgleich mit anderen Daten – angewiesen ist.[19] Der Gesetzgeber ist folglich dazu angehalten, Geheimhaltungsinteressen in einen **Ausgleich** mit dem Interesse an einer effektiven Strafverfolgung zu bringen. Allgemeine Vorgaben dafür folgen aus der JI-RL sowie aus den grundrechtlichen Eingriffsvorbehalten.

### 2. Datenschutz als Garant effektiver Strafverfolgung

Datenschutz- und Strafprozessrecht stehen jedoch nicht ausschließlich in einem Spannungsverhältnis zueinander, sondern verfolgen teilweise **gleichgerichtete Interessen.** So ist die **Geheimhaltung** von Daten aus einem Strafverfahren mitunter auch aus **ermittlungstaktischen Gründen** geboten und wird daher durch strafprozessuale Geheimhaltungspflichten eigens angeordnet.[20] Auch bei den datenschutzrechtlichen Nebenrechten zeigt sich dieser Gleichklang. Bspw dient die datenschutzrechtliche **Richtigstellung** und **Vervollständigung** auch der Strafverfolgung, weil bei der Verarbeitung unrichtiger oder unvollständiger Daten die Gefahr von Fehlschlüssen durch Ermittlungsbehörden besteht.

Selbst wenn die beiden Interessen parallel verlaufen, sind die damit verfolgten Ziele aber **genuin verschieden.** Während die Strafverfolgung primär im **öffentlichen Interesse** liegt,[21] dient das Datenschutzrecht der freien Entfaltung der Persönlichkeit und ist solcherart stets auf ein **Individuum** bezogen, den sogenannten **„Betroffenen".** Dieser kann als alleiniges Schutzobjekt auf seine datenschutzrechtlichen Geheimhaltungsrechte verzichten. Daher kann auch bei der Abschaffung der Amtsverschwiegenheit nicht völlig auf Geheimhaltungspflichten verzichtet werden, auch nicht unter Verweis auf das ohnehin bestehende Datenschutzrecht.[22]

## C. Systematik des strafprozessualen Datenschutzrechts

Die Entwicklung des strafprozessualen Datenschutzrechts fand wie bereits angesprochen auf mehreren Ebenen parallel statt, wodurch über Jahrzehnte ein komplexer normativer Rahmen entstanden ist. Daher wird zunächst die **Systematik dieses Mehrebenensystems** skizziert.

Im Zentrum der Entwicklung stand und steht **Art 8 EMRK,** der durch den EGMR zu einem umfassenden Grundrecht auf Datenschutz ausgeformt wurde und bis heute die anderen beiden Grundrechtsverbürgungen beeinflusst: **Art 8 GRC** ist mit der EMRK insofern verklammert, als das Schutzniveau der GRC nach ihrem

19 Vgl *Hornung/Schindler/Schneider*, Die Europäisierung des strafverfahrensrechtlichen Datenschutzes, ZIS 2018, 566 (566).

20 Vgl dazu das Kapitel „Offenlegung- und Veröffentlichungsverbote" S 134 ff.

21 Zu Berücksichtigung von Opferinteressen in der Straftheorie vgl aber *Schünemann*, Zur Stellung des Opfers im System der Strafrechtspflege, NStZ 1986, 193 (Teil I), 439 (Teil II); *Hörnle*, Die Rolle des Opfers in der Straftheorie und im materiellen Strafrecht, JZ 2006, 950 mN auch zu deutlich älteren Ansätzen (insb in Fn 33); vgl auch *Hassemer*, Schutzbedürftigkeit des Opfers und Strafrechtsdogmatik (1981) 22 ff, 72 ff, 79 ff.

22 In § 6 der RV zum Informationsfreiheitsgesetz sind in diesem Sinn Ausnahmen der Informationspflicht vorgesehen (RV 2238 BlgNR 27. GP).

Art 52 Abs 3 zumindest jenem der korrespondierenden EMRK-Bestimmungen entspricht.[23] Der Eingriffsvorbehalt des **§ 1 Abs 2 DSG** verweist sogar ausdrücklich auf Art 8 Abs 2 EMRK.

Auf **sekundärrechtlicher Ebene** – kompetenzrechtlich gestützt auf Art 16 Abs 2 AEUV – werden diese Vorgaben vor allem durch die DSGVO und die JI-RL näher ausgestaltet.[24] Die **DSGVO** erfasst grundsätzlich jede Verarbeitung von Daten natürlicher Personen, die automatisiert oder manuell in besonders strukturierter Form erfolgt (Art 2 Abs 1 DSGVO).[25] Nach **Art 2 Abs 2 lit d DSGVO** sind allerdings Datenverarbeitungen ausgenommen, die „durch die zuständigen Behörden 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" erfolgen. Diese Datenverarbeitungen unterliegen der **JI-RL,** deren sachlicher Anwendungsbereich (Art 1 Abs 1 JI-RL) exakt der erwähnten Ausnahme der DSGVO entspricht. Dabei kommt es nicht auf die organisatorische Einbettung der Behörde an, sondern einem „funktionalen […] Ansatz" entsprechend auf den Zweck der konkreten Verarbeitung.[26] Da es im **Strafprozess** um die „Ermittlung, Aufdeckung oder Verfolgung von Straftaten" geht, sind bei strafprozessualen Datenverarbeitungen somit grundsätzlich die JI-RL und die entsprechenden Umsetzungsbestimmungen einschlägig.[27] Dasselbe gilt für Verarbeitungen,

23 Vgl auch Art 53 GRC, wonach keine Bestimmung der GRC als Einschränkung der EMRK-Rechte ausgelegt werden darf.

24 Vom Anwendungsbereich der die elektronische Kommunikation regelnden ePrivacy-RL (Richtlinie 2002/58/EG) sind „die Tätigkeiten des Staates im strafrechtlichen Bereich" hingegen ausgenommen (Art 1 Abs 3 ePrivacy-RL). Vgl aber EuGH 21. 12. 2016, C-203/15 und C-698/15, *Tele2 Sverige*, ECLI:EU:C:2016:970 Rz 73 und 2. 10. 2018, C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788 Rz 34 f, wonach Bestimmungen iSd Art 15 ePrivacy-RL das Strafverfahren betreffend sehr wohl in den Anwendungsbereich der RL fallen; mit dem Wortlaut des Art 1 Abs 3 ist das nicht vereinbar. Vgl dazu ausführlich *Schneider*, Die Sicherstellung von Endeinrichtungen für elektronische Kommunikation im Lichte der ePrivacy-RL sowie der europäischen und österreichischen Grundrechte, in *Baumgartner* (Hrsg), Jahrbuch Öffentliches Recht 2022 (2022) 237 (242 ff).

25 Art 4 Z 2 DSGVO, Art 3 Z 2 JI-RL, § 36 Abs 2 Z 2 DSG. Zur „Datenverarbeitung" in ihren unterschiedlichen Formen vgl noch ausführlich unten bei der Begriffsdefinition S 10 f mN.

26 EBRV 1664 BlgNR 25. GP 17; vgl auch EuGH 26. 1. 2023, C-205/21, *Ministerstvo na vatreshnite raboti*, ECLI:EU:C:2023:49 Rz 61; *Bergauer*, Überblick über die österreichische Umsetzung der Richtlinie (EU) 2016/680 für den Bereich der Strafverfolgung, in *Knyrim* (Hrsg), Jahrbuch Datenschutzrecht 2017 (2017) 281 (283); *ders*, Gesetzgebungsmonitor Datenschutz: Umsetzungsentwurf der Datenschutz-Richtlinie-Strafrecht (EU) 2016/680, jusIT 2017, 158 (159); *Dörnhöfer*, Datenschutz im Strafverfolgungsbereich, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 401 (405); vgl neben der klaren Formulierung in Art 1 Abs 1 JI-RL auch ErwG 19 DSGVO.

27 *Hornung/Schindler/Schneider*, ZIS 2018, 566 (568 f); *Kristoferitsch/Bugelnig* in WK StPO § 74 Rz 4 ff; *Dörnhöfer* in *Knyrim*, Datenschutz-Grundverordnung 401 (404). Zur Anwendbarkeit auf gerichtliche Datenverarbeitungen vgl *Cepic/Gilhofer*, Die Löschung von rechtswidrig ermittelten personenbezogenen Daten in der Strafrechtspflege – Ein- und Auswirkungen von § 75 StPO, JBl 2023, 409 (410).

die der „Verhütung" von Straftaten dienen. Die JI-RL erfasst daher auch einige nach genuin österreichischem Verständnis **sicherheitspolizeiliche** Tätigkeiten.[28]

Bei **Grenzfällen** zwischen DSGVO und JI-RL ist anhand einer **autonomen Interpretation des Sekundärrechts** eine Zuordnung vorzunehmen.[29] Bspw kann beim Fund einer Leiche zunächst unklar sein, ob ein Geschehen einen Zusammenhang zum Verdacht einer **„Straftat"** aufweist.[30] In diesem Übergangsbereich ist nach ErwG 12 die JI-RL relevant, sodass sich die Grenzen der Datenverarbeitung aus den nationalen Umsetzungsbestimmungen ergeben.[31] Hingegen ist die DSGVO anwendbar, wenn eine Datenverarbeitung zwar inhaltlich mit dem Strafprozess zusammenhängt, aber **nicht unmittelbar** der Verhütung, Verfolgung oder Vollstreckung im oben genannten Sinn dient.[32] Das betrifft etwa die gesamte Justizverwaltung,[33] die Übermittlung von im Strafverfahren erhobenen Daten an sonstige Behörden,[34] „die Verteidigung des Staates gegenüber einer" Amtshaftungsklage eine Handlung der StA betreffend,[35] die Führung des Strafregisters[36] sowie die Medienarbeit der Strafverfolgungsbehörden[37].

Nicht in den Anwendungsbereich der beiden Rechtsakte fallen alle **manuellen, nicht-systematisierten Verarbeitungen.** Als Bsp hierfür wird in den ErwG 18 JI-RL sowie 15 DSGVO die Führung eines **Papieraktes** genannt, da die bloße Beschriftung des Aktendeckels noch keine ausreichende Systematisierung iS eines Dateisystems darstellt.[38] Anders ist es aber, wenn die Akten einer Behörde nach allgemeinen Kriterien – etwa dem Namen einer Verfahrenspartei oder einer Geschäftszahl – geordnet

28 Vgl *Dörnhöfer* in *Knyrim*, Datenschutz-Grundverordnung 401 (405); *Pichler*, Die Umsetzung der RL 2016/680 und deren Auswirkungen auf das Straf- und Strafprozessrecht, in *Landesgruppe Österreich der AIDP/Österreichischer Juristenverband* (Hrsg), Der neue Datenschutz (2018) 33 (35).

29 Vgl nur ErwG 13 JI-RL.

30 EBRV 1664 BlgNR 25. GP 16; *Pichler* in *Landesgruppe Österreich der AIDP/Österreichischer Juristenverband*, Datenschutz 33 (36 f).

31 Vgl EuGH 8. 12. 2022, C-180/21, *Inspektor*, ECLI:EU:C:2022:967 Rz 58; vgl auch *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz (2018) Rz 22; *Dörnhöfer* in *Knyrim*, Datenschutz-Grundverordnung 401 (405). Die Verarbeitung von Daten des Verstorbenen selbst unterliegt allerdings nicht dem Datenschutzrecht; vgl nur ErwG 27 DSGVO.

32 Vgl zur Abgrenzung auch *Divjak*, Anmerkung zu EuGH 8. 12. 2022, C-180/21, *Inspektor*, ECLI:EU:C:2022:967, jusIT 2023, 150.

33 *Kristoferitsch/Bugelnig* in WK StPO § 74 Rz 5; *Dörnhöfer* in *Knyrim*, Datenschutz-Grundverordnung 401 (404).

34 EuGH 22. 6. 2021, C-439/19, *Latvijas Republikas Saeima*, ECLI:EU:C:2021:504 Rz 61, 69 ff; vgl auch ausführlich unten im Kapitel zur „Beschränkung der Datenübermittlung" S 157 ff.

35 EuGH 8. 12. 2022, C-180/21, *Inspektor*, ECLI:EU:C:2022:967 Rz 64 ff (insb 78 f).

36 Vgl nur § 1 Abs 2 Strafregistergesetz 1968.

37 Dazu ausführlich unten im Kapitel „Offenlegungs- und Veröffentlichungsverbote" S 134 ff.

38 Vgl dazu auch *Johannes/Weinhold*, Datenschutzrecht Rz 18; *Heißl* in *Knyrim*, DatKomm Art 2 DSGVO Rz 54; *Feiler/Forgó*, EU-DSGVO und DSG² (2022) Art 2 Rz 6; *Kristoferitsch/Bugelnig* in WK StPO § 74 Rz 20; *Hladjk*, Sachlicher und räumlicher Anwendungs-

werden, da hier ein zielgerichtetes Auffinden der Daten möglich ist.[39] Da sämtlichen Akten im Strafverfahren ein systematisch gebildetes Aktenzeichen zugeordnet ist (§§ 371 ff Geo., § 8a Abs 10 DV-StAG), unterliegt die Führung des Papieraktes der JI-RL.[40] Wird der Akt elektronisch geführt, liegt eine automatisierte Verarbeitung vor.[41]

Die **Umsetzung** der JI-RL erfolgt im Bereich des Strafverfahrens primär durch die **StPO.** Da der Gesetzgeber in der StPO allerdings nur ganz vereinzelt spezifisch datenschutzrechtliche Vorschriften vorgesehen hat, muss hier idR versucht werden, klassisch strafprozessuale Bestimmungen richtlinienkonform auszulegen. Bspw findet die datenschutzrechtliche Auskunft grundsätzlich im Rahmen der strafprozessualen Akteneinsicht statt.[42] Daneben sieht das **3. HS des DSG** detaillierte Regelungen zur Datenverarbeitung im Strafprozess vor. Diese Bestimmungen kommen gem § 74 Abs 1 zweiter Satz[43] jedoch iSe datenschutzrechtlichen Sicherheitsnetzes nur **subsidiär** zur Anwendung, sofern in der StPO „nichts anderes bestimmt wird". Das trifft zum einen zu, wenn die StPO zu einem Teilbereich überhaupt keine Regelungen enthält, etwa hinsichtlich der meisten Fragen der Datensicherheit.[44] Zum anderen ist das DSG auch anzuwenden, wenn sich ein nach der JI-RL zwingendes Auslegungsergebnis nur so erzielen lässt. In richtlinienkonformer Interpretation des § 74 Abs 1 zweiter Satz bestimmt das DSG hier „anderes", selbst wenn die StPO den Fall auch (allerdings unzureichend) regelt. Das betrifft zB die DSG-Regelungen zur Auskunft und Information gem § 44 Abs 1 DSG, sofern die entsprechenden Informationen nicht im Wege der Akteneinsicht ersichtlich sind (bspw Informationen, für welche Dauer die Daten voraussichtlich gespeichert werden und an wen sie übermittelt wurden).[45]

---

bereich der DSGVO, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 39 (40) jeweils mwN.

39 Vgl erneut ErwG 18 JI-RL und ErwG 15 DSGVO. Dazu auch *Schild* in *Wolff/Brink/v. Ungern-Sternberg*, BeckOK Datenschutzrecht[44] Art 4 DSGVO Rz 83 ff (Stand: 1. 5. 2023); *Ernst* in *Paal/Pauly*, DS-GVO BDSG[3] Art 4 Rz 54.

40 *Cepic/Gilhofer*, JBl 2023, 409 (412 f) mN; *Kristoferitsch/Bugelnig* in WK StPO § 74 Rz 20; zu Gerichtsakten vgl außerdem VG München 13. 7. 2021, M 32 K 20.6162 (Nachweis bei *Schild* in *Wolff/Brink/v. Ungern-Sternberg*, BeckOK Datenschutzrecht[44] Art 4 DSGVO Rz 83 [Stand: 1. 5. 2023]). Die Speicherung im elektronischen Akt findet – als automatisierte Datenverarbeitung – ohnehin im Anwendungsbereich der JI-RL statt.

41 Zur geplanten flächendeckenden Einführung der elektronischen Aktenführung vgl das Regierungsprogramm der österreichischen Bundesregierung (2020) 23; zum Zivilverfahren ausführlich *Spiegel*, ZVN 2022: Digitalisierung im Zivilverfahren, ecolex 2022, 614.

42 Vgl dazu ausführlich unten im Kapitel zur „Auskunft und Information" S 110 ff.

43 Sofern nichts anderes angeführt ist, beziehen sich alle §§-Verweise auf die StPO.

44 Vgl EBRV 65 BlgNR 25. GP 164, wonach der Vorrang der StPO „generalisierend" wirkt; dazu auch OGH 10. 12. 2019, 11 Os 76/19i. Zur Datensicherheit vgl das eigene Kapitel dazu S 195 ff.

45 Dazu ausführlich S 111 ff.

Konkretisiert werden die gesetzlichen Vorgaben durch zahlreiche **Erlässe der BMJ** (BMVRDJ) sowie des **BMI,**[46] insb durch den Datenschutz-Erlass,[47] den Erlass zur Zulässigkeit von VJ-Abfragen[48] und Medien-Erlässe[49]. Im vorliegenden Zusammenhang ist allerdings fraglich, ob Erlässe ein geeignetes Mittel zur Umsetzung der JI-RL sind. Hinsichtlich der **Rechtsprechung** kann dies von vornherein verneint werden, da sich Erlässe nicht auf die eigentliche gerichtliche Tätigkeit beziehen.[50] Der typische Zusatz „unvorgreiflich der Rechtsauffassung der unabhängigen Gerichte" stellt dies nochmals klar. Organe der StA sowie der Kripo sind zwar grundsätzlich weisungsgebunden (Art 90a B-VG, § 2 Abs 1 StAG bzw Art 20 Abs 1 B-VG). Dennoch kommt eine erlassförmige Umsetzung der JI-RL auch hier nicht in Betracht. So ist die Umsetzung unionsrechtlich zwingend so auszugestalten, dass der Betroffene die Rechtmäßigkeit der Verarbeitung bei Gericht durchsetzen kann (Art 52, 54 JI-RL).[51] Da Erlässe allerdings kein Prüfungsmaßstab im Einspruchsverfahren (§ 106 Abs 1) sind,[52] bestünde bei einer solchen Umsetzung keine Möglichkeit für den Betroffenen, die Einhaltung der Verarbeitungsbedingungen gerichtlich durchzusetzen. Der Zweck des Erlasses besteht somit in der internen Bindung der Organe und der dadurch ermöglichten einheitlichen Vollziehung, ausreichend bestimmte **gesetzliche Vorgaben** zur Datenverarbeitung ersetzt der Erlass aber nicht.

46 Diese können aufgrund ihres Inhalts entweder als generelle Weisung (Art 20 Abs 1 B-VG) oder – sofern sie die Rechtsstellung Einzelner gestalten und damit Außenwirkung haben – als Verordnung (Art 18 Abs 2 B-VG) qualifiziert werden; vgl VfGH 23. 6. 2021, V95/2021 ua; VfSlg 17.849/2006; 15.061/1997; 12.744/1991; dazu auch *Grabenwarter/Holoubek*, Verfassungsrecht – Allgemeines Verwaltungsrecht[5] (2022) Rz 976; *Berka*, Verfassungsrecht[8] (2021) Rz 669.

47 Erlass des BMVRDJ (nunmehr: BMJ) vom 24. 4. 2018, BMVRDJ-Pr6116/0006-III 3/2018 („Datenschutz-Erlass").

48 Erlass des BMJ vom 20. 8. 2015, BMJ-V225.01/0008-III 5/2015 (Zulässigkeit von VJ-Abfragen, Begründungspflichten und die Folgen eines Missbrauchs).

49 Erlass des BMJ vom 23. 5. 2016, BMJ-Pr50000/0021-Kom/2016 (Zusammenarbeit mit den Medien); der aktuelle Medienerlass des BMI wurde nach einer schriftlichen Anfrage „aus Datenschutzgründen" nicht zur Verfügung gestellt.

50 Eine solche generelle Bindung der Gerichtsbarkeit an Akte eines Verwaltungsorgans stünde in Widerspruch zum gewaltenteilenden Grundprinzip. Im Rahmen der monokratischen Justizverwaltung besteht zwar eine Weisungsbindung (Art 87 Abs 2 B-VG), allerdings ist die JI-RL bei Tätigkeiten der Justizverwaltung wie erwähnt generell nicht anwendbar.

51 Dazu *Divjak*, Die Durchsetzung von Datenschutzrechten im Ermittlungsverfahren, JBl 2022, 489 (491 ff).

52 Vgl *Pilnacek/Stricker* in WK StPO § 106 Rz 11 ff.

# D. Grundbegriffe des Datenschutzrechts

## 1. Datum

Ein **„Datum"** ist jede **Darstellung einer Information,**[53] die für den Menschen – ggf mithilfe technischer Geräte – **lesbar** ist.[54] Ein Datum liegt daher etwa vor, wenn eine Information schriftlich auf Papier festgehalten wird, da durch die Interpretation dieser Darstellung auf die repräsentierte Information geschlossen werden kann (sog **„Abstraktion"**).[55] Die „Lesbarkeit" von Daten ist dabei nicht notwendigerweise auf geschriebene Sprache bezogen, sondern meint jede **Erfassbarkeit eines Inhalts,** womit auch Ton- und Videoaufnahmen erfasst sind. Bloße Gedanken sind hingegen – weil für andere nicht lesbar – keine Daten.[56]

In der **Informatik** erfolgt die Darstellung von Informationen durch vorgegebene Zeichen (meist im Dualsystem durch Einser und Nullen), wodurch eine maschinelle Verarbeitung möglich wird.[57] Entsprechende Speichermedien sind Festplatten, USB-Sticks, CD und DVD. Diese Form der Darstellung ist praktisch besonders bedeutsam; der Begriff des „Datums" ist aber nicht auf sie beschränkt, sondern bezieht sich technikunabhängig auf **jede Form der lesbaren Repräsentation.**[58]

## 2. Besondere Kategorien personenbezogener Daten

Als **„besondere Kategorien personenbezogener Daten"** werden in JI-RL und DSGVO Daten bezeichnet, die insb aufgrund ihres Inhalts **besonders sensibel sind** und daher **besonderen Verarbeitungsbedingungen unterliegen** (Art 10 JI-RL, Art 9 Abs 1 DSGVO).[59] Dazu zählen etwa Daten zur ethnischen Herkunft, zu religiösen

53 Zum umfassenden Begriff der „Information", der jeden denkbaren „Sinngehalt" umfasst, vgl *Albers*, Informationelle Selbstbestimmung (2015) 87 ff mN; *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO Rz 9; *Klar/Kühling* in *Kühling/Buchner*, DSGVO/BDSG[2] Art 4 Nr 1 DSGVO Rz 8 ff.

54 Vgl *Zilahi-Szabó*, Informatik[3] (1998) 21 ff (insb 23); *Gumm/Sommer*, Einführung in die Informatik[10] (2013) 4; *Bergauer*, Das materielle Computerstrafrecht (2016) 67; *ders*, Personenbezogene Daten, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 43 (43 f); *Haidinger*, Grundbegriffe und Definitionen, in *Knyrim* (Hrsg), Datenschutzrecht[4] (2020) Rz 3.14 ff; *Cepic/Gilhofer*, JBl 2023, 409 (411); *Albers*, Selbstbestimmung 89 mwN (insb in Fn 233); *Hampel*, Der Datenbegriff im Strafgesetzbuch (2015) 7 ff; vgl auch den internationalen Technologiestandard ISO/IEC 2382:2015, 2121272.

55 Vgl *Gumm/Sommer*, Einführung[10] 4; *Bergauer*, Computerstrafrecht 62, 67.

56 *Ennöckl*, Privatsphäre 122 ff; vgl auch *Bergauer*, Personenbezogene Daten, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 43 (43 f); differenzierend *Eberhard* in *Korinek/Holoubek* ua, Bundesverfassungsrecht § 1 DSG Rz 30.

57 *Gumm/Sommer*, Einführung[10] 4 f; *König/Pfeiffer-Bohnen/Schmeck*, Theoretische Informatik – ganz praktisch (2016) 2 ff; *Warnke*, Informatik[2] (1991) 23 f; vgl auch Art 1 lit b Cyber-Crime Konvention; *Reindl-Krauskopf* in WK StGB[2] § 74 Rz 65.

58 Vgl *Bergauer*, Computerstrafrecht 61 ff; *Ennöckl*, Privatsphäre 125; *Schild* in *Wolff/Brink/v. Ungern-Sternberg*, BeckOK Datenschutzrecht[44] Art 4 DSGVO Rz 42 (Stand: 1. 5. 2023).

59 Dazu ausführlich *Haidinger* in *Knyrim*, Datenschutzrecht[4] Rz 3.21 ff. Zu den Kriterien vgl EuGH 1. 8. 2022, C-184/20, *Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601 Rz 117 ff.

Überzeugungen, zur sexuellen Orientierung, zum Gesundheitszustand sowie biometrische Daten. Gerade im Strafverfahren wird häufig auf solche Daten zugegriffen. So ermöglichen die auf einem sichergestellten Smartphone gespeicherten Daten regelmäßig Rückschlüsse auf den Gesundheitszustand des Inhabers (etwa durch abgespeicherte Blutbefunde und Suchverläufe), die sexuelle Orientierung (Nachrichten in einer Dating-App) sowie die religiösen und weltanschaulichen Überzeugungen (Textnachrichten an Gleichgesinnte, Fotos, Screenshots).

## 3. Personenbezug und Betroffener

**Schutzobjekt** des Datenschutzrechts ist nicht das Datum als solches, sondern stets eine **Person,** auf die sich das Datum inhaltlich bezieht.[60] Diese Verbindung zwischen dem Datum und der Person wird als **„Personenbezug"** bezeichnet, die Person als **„Betroffener".** Dabei reicht es aus, wenn die Person unter Einsatz aller „nach allgemeinem Ermessen wahrscheinlich" genutzter technischer Mittel **identifizierbar** ist.[61] Eine tatsächliche Kenntnis ist somit nicht erforderlich. Die Verarbeitung von Daten ohne Personenbezug unterliegt nicht dem Datenschutzrecht.[62]

## 4. Verarbeitung

Datenschutzrechtliche Vorschriften knüpfen in ihrem sachlichen Anwendungsbereich typischerweise an die **„Verarbeitung"** von Daten an. Darunter fällt in einem weiten Sinn nahezu **jeder auf Daten bezogene Vorgang,** etwa das Erheben, Ordnen, Speichern, Abfragen, Übermitteln und Löschen.[63] Selbst das bloße Aufbewahren eines Datenträgers in einem Archiv wird als Datenverarbeitung gewertet, auch wenn zu keinem Zeitpunkt tatsächlich auf die Daten zugegriffen wird.[64] Das bloße Empfangen von Daten ohne eigenes Zutun kann hingegen begrifflich nicht als „Verar-

60 *Klabunde* in *Ehmann/Selmayr*, Datenschutz-Grundverordnung[2] Art 4 Rz 7; *Jahnel/Pallwein-Prettner*, Datenschutzrecht[3] (2021) 15.

61 Vgl Art 3 Z 2, ErwG 21 JI-RL; Art 4 Z 1, ErwG 26 DSGVO; grundlegend zur (aufgehobenen) Datenschutz-RL EuGH 19. 10. 2016, C-582/14, *Breyer*, ECLI:EU:C:2016:779 Rz 31 ff; vgl auch *Klar/Kühling* in *Kühling/Buchner*, DSGVO/BDSG[2] Art 4 Nr 1 DSGVO Rz 17 ff; *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO Rz 12 ff; *Bergauer* in *Knyrim*, Datenschutz-Grundverordnung 43 (53 ff); *Salimi* in WK StGB[2] § 63 DSG Rz 26 f; *Rohregger* in LK StPO § 74 Rz 7; *Cepic*, Zur Antragstellung auf (nachträgliche) Anonymisierung und zur Anonymisierungsmethodik bei Entscheidungen des OGH, jusIT 2021, 160 (162 f) sowie das Kapitel zur „Anonymisierung" S 75 ff.

62 ErwG 21 JI-RL; vgl auch *Salimi* in WK StGB[2] § 63 DSG Rz 29; *Bergauer* in *Knyrim*, Datenschutz-Grundverordnung 43 (47).

63 Vgl Art 3 Z 2 JI-RL; Art 4 Abs 2 DSGVO; dazu ausführlich *Roßnagel* in *Simitis/Hornung/Spiecker*, Datenschutzrecht Art 4 Nr 2 DSGVO Rz 10 ff; *Herbst* in *Kühling/Buchner*, DSGVO/BDSG[2] Art 4 Nr 2 DSGVO Rz 11 ff; *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO Rz 25 ff; *Lachmayer* in *Knyrim*, DatKomm § 36 DSG Rz 19; vgl auch schon *Divjak*, Das gerichtliche Datenschutzstrafrecht, ÖJZ 2023, 650.

64 *Schild* in *Wolff/Brink/v. Ungern-Sternberg*, BeckOK Datenschutzrecht[44] Art 4 DSGVO Rz 42a (Stand: 1. 5. 2023); *Herbst* in *Kühling/Buchner*, DSGVO/BDSG[2] Art 4 Nr 2 DSGVO Rz 24.