Hochschule Hof
University of Applied Sciences

Hofer akademische Schriften

zum Recht in Nachhaltigkeit, Compliance und IT

Herausgegeben von Prof. Dr. Beatrix Weber

Band 4

Jan Valentin Baumgärtner

Die Verarbeitung personenbezogener Daten bei polizeilichen Maßnahmen im Rahmen strafrechtlicher Ermittlungen aufgrund einer Einwilligung des Betroffenen

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der deutschen Nationalbibliografie;detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Hofer akademische Schriften zum Recht in Nachhaltigkeit, Compliance und IT
Herausgegeben von Prof. Dr. Beatrix Weber
Professorin für Gewerblichen Rechtssschutz und IT-Recht an der Hochschule Hof / University of Applied Sciences

Band 4

Jan Valentin Baumgärtner

Die Verarbeitung personenbezogener Daten bei polizeilichen Maßnahmen im Rahmen strafrechtlicher Ermittlungen aufgrund einer Einwilligung des Betroffenen

Der vorliegende Text wurde ursprünglich im Wintersemester 2023/2024 als Masterarbeit an der Hochschule für angewandte Wissenschaften Hof, Studienfakultät für Weiterbildung, Studiengang Master Compliance, IT und Datenschutz, eingereicht und betreut durch Rechtsanwältin Stephanie Hofmann.

Druck und Verlag:
Hochschule Hof, Studienfakultät für Weiterbildung, Alfons-Goppel-Platz 1, D-95028 Hof

ISBN 978-3-935565-40-0
https://doi.org/10.57944/1051-182

Die Verarbeitung personenbezogener Daten bei polizeilichen Maßnahmen im Rahmen strafrechtlicher Ermittlungen aufgrund einer Einwilligung des Betroffenen

Eine Analyse der datenschutzrechtlichen Voraussetzungen

Masterthesis

an der Hochschule für angewandte Wissenschaften Hof

Masterstudiengang Compliance, IT und Datenschutz Forschung

vorgelegt bei
RA Frau Hofmann
Alfons-Goppel-Platz 1
95028 Hof

vorgelegt von
Jan Baumgärtner
Kronprinzendamm 4
10711 Berlin

Berlin, 30.10.2023

Inhaltsverzeichnis

Abkürzungsverzeichnis

Sofern die Abkürzungen nicht besonders erläutert werden, wird verwiesen auf:

Kirchner, Hildebert / Pannier, Dietrich, Abkürzungsverzeichnis der Rechtssprache, 10. Auflage, Berlin, 2021

A. Einleitung

Jeden Tag finden in Deutschland zahlreiche allgemeine und anlassbezogene Verkehrskontrollen durch die Polizei und andere Kontrollbehörden statt. Nicht selten wird Angehaltenen nebst der Prüfung der mitzuführenden Dokumente auch noch angeboten einen Atemalkoholtest durchzuführen oder mit den Kontrollbeamten einige andere Tests zur Sicherstellung der Fahrtauglichkeit zu absolvieren.

Besteht für den Kontrollierten zwar die Pflicht Angaben zu seiner Person zu machen und auf Nachfrage der Polizisten, einen Nachweis über seine Fahrerlaubnis und die Zulassungsbescheinigung Teil II vorzuzeigen, ist dieser aber dabei grundsätzlich frei in seiner Entscheidung, was die Zustimmung zu angebotenen Tests und seiner aktiven Mitwirkung an solchen angeht.

Eine solche Freiwilligkeit der aktiven oder passiven Mitwirkung gibt es auch bei anderen polizeilichen Maßnahmen, wie etwa der Entnahme einer DNS-Probe, es sei denn, dass die Maßnahme aufgrund eines Beschuldigtenstatus angeordnet oder durchgeführt werden kann.

Wird eine Probe entnommen oder ein Test durchgeführt, so können hieraus gewonnene Erkenntnisse auch im Rahmen eines Ermittlungsverfahrens zu einem ordentlichen Strafprozess führen.

Gleichwohl einer vorliegenden Einwilligung bleibt die Durchführung eines Tests oder die Entnahme einer Probe auch immer eine Verarbeitung von personenbezogenen Daten des Betroffenen. Eine solche Verarbeitung hat abgesehen von den Rechtsgrundlagen für die Durchführung polizeilicher Maßnahmen auch immer die Belange des Datenschutzes - als von der Union gewährtes Grundrecht[1] – zu berücksichtigen. Genau wie auch etwa ein staatlicher Eingriff in die körperliche Unversehrtheit bedarf auch eine Verarbeitung personenbezogener Daten durch staatliche Behörden immer einer Rechtsgrundlage. Gerechtfertigt kann eine solche Verarbeitung stets nur

[1] Art. 8 Abs. 1 GrCH

sein, wenn im Rahmen der bestehenden Gesetze eine solche Eingriffsgrundlage gegeben ist und diese auch dem Grundsatz der Verhältnismäßigkeit entspricht.

Existiert eine solche Rechtsgrundlage und ist die dadurch legitimierte Verarbeitung auch verhältnismäßig, ist dennoch zu prüfen, ob auch alle Voraussetzungen der Rechtsgrundlage erfüllt wurden. Im Falle der Einwilligung ist es beispielsweise nicht ausreichend, dass ein Betroffener der Durchführung einer Maßnahme formal zustimmt, nach dem dieser dazu befragt wurde. Der Betroffene muss vielmehr konkret wissen, welche seiner Daten erfasst werden und wie diese im Weiteren zu welchen Zwecken und durch welche Stelle verarbeitet werden. Fehlt es dem Betroffenen an einer Information, so kann es möglicherweise zu Fehlern bei der Willensbildung kommen und der Betroffene willigt in eine Maßnahme ein, in welche er bei Vorliegen aller Informationen, seine Zustimmung verweigert hätte.

Fraglich ist aber auch unter welchen Umständen ein von einer polizeilichen Maßnahme – etwa im Rahmen einer Kontrollsituation – Betroffener überhaupt die Möglichkeit hat hierin einzuwilligen. Zu beleuchten ist hier, ob diese Möglichkeit gesetzlich explizit verankert sein muss, oder es Betroffenen grundsätzlich möglich sein kann in sämtliche von der Polizei angebotene oder angesetzte Maßnahmen einzuwilligen, bzw. wo die Grenzen einer solchen Einwilligung vorliegen.

Die vorliegende Arbeit untersucht die genauen Voraussetzungen einer datenschutzrechtlichen Einwilligung betroffener Personen, die sich im aufgrund polizeilicher Ermittlungen, die im Rahmen von strafprozessualen Maßnahmen durchgeführt werden. Dabei wird insbesondere auf die genauen Tatbestandsmerkmale einer Einwilligung Bezug genommen, mit dem Ziel herauszustellen, welche dieser Merkmale notwendig sind, um eine datenschutzrechtliche Einwilligung sicher anzunehmen. Des Weiteren wird analysiert, unter welchen rechtlichen Bedingungen es einem Betroffenen offensteht, in eine Verarbeitung einzuwilligen.

Bei der Beurteilung der Einwilligung liegt der Fokus auf der Beurteilung unmittelbarer datenschutzrechtlicher Probleme. Andere Aspekte, wie etwa die Einwilligungsmöglichkeit der Beeinträchtigung anderer Grundrechte werden bei Relevanz am Rande berücksichtigt, zählen aber nicht zum Kerngegenstand der vorliegenden Arbeit.

Nicht Bestandteil der Arbeit ist ebenfalls die Einschätzung einer mögliche Beweiswürdigung der vom Betroffenen erfassten Daten, zu welchen dieser möglicherweise keine ausreichende Einwilligung abgegeben hat.

Die Arbeit stellt nach einer historischen Einordnung zunächst das Verhältnis zwischen EU-Datenschutzgrundverordnung und Bundesdatenschutzgesetz dar und erklärt grundlegende Komponenten, um die Fallfrage zu erörtern. Nach Klärung der Anwendbarkeit der Gesetzgebung werden zunächst die Einhaltung der Datenschutzgrundsätze überprüft, da diese essenziell für jegliche Verarbeitung personenbezogener Daten ist und widmet sich anschließend der Thematik der Erfüllung aller Voraussetzungen für das Vorliegen einer wirksamen Einwilligung im Kontext strafprozessualer Maßnahmen. Die Ergebnisse werden abschließend noch einmal im Fazit kurz zusammengefasst.

Aufgrund der vielfachen inhaltlichen Überschneidung zwischen Bundesdatenschutzgesetz und EU-Datenschutzgrundverordnung wird vielmals auch auf die entsprechenden Kommentierungen und Aufsätze zur DSGVO zurückgegriffen, um Erläuterungen der Vorschriften des BDSG zu bieten, wobei vorliegende Unterschiede natürlich Berücksichtigung finden. Zur weiteren Bearbeitung der Fallfrage werden außerdem juristische Auslegungsmethoden, wie die systematische oder teleologische Auslegung angewandt und andere methodische Werkzeuge wie der Erst-Recht-Schluss oder der Umkehrschluss verwendet.

B. Historische Einordnung

Als am 25. Mai 2018 die „Verordnung (EU) 2016/679“, im offiziellen Sprachgebrauch als „EU-Datenschutzgrundverordnung“[2] bezeichnet, in Kraft trat, wurde damit erstmalig eine innerhalb der Europäischen Union harmonisierte Rechtsverordnung zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogenen Daten implementiert. Der von der DSGVO abgelöste Vorgänger war die von der EU erlassene Richtlinie „95/46/EG zum Schutz natürlicher personenbezogener Daten und zum freien Datenverkehr“[3] aus dem Jahre 1995, welche innerhalb von 3 Jahren in nationales Recht umzusetzen war. Die deutsche Legislative verabschiedete, erst nach Ablauf der Umsetzungsfrist im Jahre 2001, daraufhin das „Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze“[4], welche vor allem das Bundesdatenschutzgesetz umfassend den Vorgaben der Richtlinie anglich.

Von der Regelungskompetenz der Datenschutzrichtlinie nicht umfasst war gemäß Art. 3 Abs. 2 erster Spiegelstrich die Verarbeitung personenbezogener Daten durch staatliche Stellen im Bereich des Strafrechts. Vielmehr galt als Grundlage für die Verarbeitung personenbezogener Daten auf diesem Gebiet der „Rahmenbeschluss 2008/977/JU“[5] des Rates der Europäischen Union, welcher das Schutzniveau im Rahmen polizeilicher und justizieller Zusammenarbeit bestimmt. Dies änderte sich auch mit Einführung der DSGVO nicht, bei dem nach Art. 2 Abs. 2 lit. d) der sachliche Anwendungsbereich bei der Verarbeitung von Daten mit Personenbezug im Kontext strafjustizieller Maßnahmen ebenfalls nicht eröffnet wird. Im Kontext der Neunovellierung des europaweiten Datenschutzrechts wurde jedoch auch

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE; abgerufen am 29.12.2022
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046&from=DE; abgerufen am 29.12.2022
[4] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl101s0904.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl101s0904.pdf%27%5D__1672298970277; abgerufen am 29.12.2022
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02008F0977-20081230&from=EN; abgerufen am 29.12.2022

der Rahmenbeschluss durch die erlassene „Richtlinie (EU) 2016/680“ ersetzt[6] (JI-Richtlinie), welche das Ziel hat, ein der DSGVO ebenbürtiges Schutzniveau auch für Verarbeitungen von Strafverfolgungsbehörden zu schaffen, dass von den EU-Mitgliedsstaaten entsprechend in nationales Recht umgesetzt werden muss. Die Verabschiedung der Richtlinie im Jahre 2016 und Umsetzungsfrist dieser bis Mai 2018 entsprechen dabei dem gleichen Zeitraum, in welches der EU-Gesetzgeber für Verabschiedung und Inkrafttreten der DSGVO vorgesehen hat.[7] Beiden Rechtsnormen dienen dabei unmittelbar der Wahrung des Grundrechts auf den Schutz personenbezogener Daten, welcher durch Art. 8 Abs. 1 GrCh, bzw. Art. 16 Abs. 1 AEUV seitens der Europäischen Union kodifiziert gewährleistet wird.[8]

Die Gründe für den Schutz personenbezogener Daten im Justiz- und Strafsachenkontext spezifischere Regelungen zu treffen, ergeben sich nach Erklärung Nr. 21 der Regierungskonferenz danach aus dem besonderen Charakter dieser Bereiche.[9] Dazu zählt etwa auch die multiliterale Vernetzung der Justizbehörden, um letztendlich eine effizientere Strafverfolgung zu erreichen, welche schon 2004 im vom Europäischen Rat angenommen „Haager Programm (2005/C 53/01)“[10] als Ziel ausgegeben wurde.[11]

Aufgrund der Unterschiede in den einzelnen Rechtssystemen und der Wahrung der einzelstaatlichen Kompetenzen in diesem Zusammenhang fiel die Wahl zur Schaffung eines Mindestharmonisierungsstandards[12] auf eine Richtlinie und nicht auf eine Verordnung.[13] Dabei dienen die in

[6] vgl. Art. 59 Abs. 1 JI-RL, ErwG 6 JI-RL
[7] vgl. Art. 63 Abs. 1 JI-RL, Umsetzung bis 6. Mai 2018 bei Verabschiedung der Norm am 27. April 2016, Veröffentlichung im Amtsblatt der EU am 04.05.2016; vgl. Art. 99 Abs. 2 DSGVO, Inkrafttreten ab 25. Mai 2018; Verabschiedung ebenfalls am 27.April 2016, Veröffentlich im Amtsblatt der EU am 04.05.2016
[8] vgl. ErwG 1 JI-RL; ErwG 1 DSGVO
[9] https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0004.01/DOC_6&format=PDF; abgerufen am 29.12.2022
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52005XG0303(01)&from=DE; abgerufen am: 29.12.2022
[11] vgl. Punkt 3.3 Haager Programm
[12] vgl. ErwG 15 JI-RL
[13] Sydow in Sydow/Marsch, DS-GVO|BDSG, Einleitung Rn. 85

der JI-Richtlinie enthaltenen Regelungen dem Wortlaut nach gem. Art. 1 Abs. 1 dem „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung“, was auch den „Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit“ einschließt.[14]

Der deutsche Gesetzgeber folgte der Pflicht zur Umsetzung dieses Mal fast fristgemäß und kodifizierte die in der JI-Richtlinie enthaltenen Regelungsvorgaben im dritten Teil der Neufassung des Bundesdatenschutzgesetzes, welches gleichermaßen zur DSGVO am 25. Mai 2018 in Kraft trat. Das dafür notwendige Änderungsgesetz „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680“ (DSAnpUG-EU) wurde bereits ein Jahr zuvor beschlossen und verabschiedet.[15]

C. Verhältnis JI-Richtlinie/DSGVO

Um das Zusammenspiel von JI-Richtlinie und DSGVO, vor allem aber auch deren Abgrenzung zueinander zu verstehen, ist es notwendig das Verhältnis beider kurz zu erörtern.

Strukturell gesehen gleichen sich die JI-Richtlinie und die DSGVO. Zehn der elf Kapitel der DSGVO finden sich mit Regelungsgeboten auch innerhalb der JI-Richtlinie wieder. Auch definitorisch finden sich inhaltsgleiche Begriffsbestimmungen in beiden Normen wieder[16], so dass von einer einheitlichen Terminologie ausgegangen werden kann.[17] Der Schutzgegenstand sowohl der DSGVO in Art. 1 Abs. 1 als auch der JI-

[14] vgl. ErwG 11 JI-RL
[15] Verabschiedung am 30. Juni 2017, Veröffentlichung im Bundesanzeiger am 5. Juli 2017; https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id=%27bgbl117s2097.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1672409477055, abgerufen am 30.12.2022
[16] vgl. Art. 4 DSGVO; Art. 3. JI-RL
[17] Lauber-Rönsberg in Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, Rn. 18

RL in Art. 1 Abs. 1 ist insofern deckungsgleich, als dass beide EU-Rechtsakte sich dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten verpflichten. Hinsichtlich des Anwendungsbereiches knüpft die JI-Richtlinie in Art. 2 Abs. 1, Art. 1 Abs. 1 dort an, wo die DSGVO diesen in Art. 2 Abs. 2 lit. d) explizit nicht eröffnet, der Datenverarbeitung durch Behörden im Kontext strafrechtlicher Angelegenheiten, deren Zuständigkeit vorausgesetzt. Der Wortlaut beider Rechtsnormen stellt indes die Zwecke der Verhütung, der Ermittlung, der Aufdeckung und der Verfolgung von Straftaten als diejenigen dar, an welchen eine solche strafrechtskontextuelle Verarbeitung bemessen werden soll. Ebenfalls adressiert werden Verarbeitungen für strafvollstreckende Zwecke, ohne diese jedoch analog zu den zuvor aufgeführten straftatenbezogenen Zwecken, zu untergliedern. Der deutsche Gesetzgeber hingegen impliziert die Strafvollstreckung im BDSG ergänzend zu Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten durch die begriffliche Addition der Ahndung. Auch hinsichtlich des von der DSGVO von der eigenen Anwendung abgelehnten Zweck der Gefahrenabwehr bedient sich die deutsche Legislative nicht der Übernahme des Richtlinien-Passus, sondern subsumiert die Gefahrenabwehr in §45 S. 3 unter die Verhütung. Führt eine zuständige Behörde Verarbeitungen durch, welchen keinem dieser Zwecke dienen, so ist aber wiederrum die Anwendung der JI-Richtlinie ausgeschlossen und die DSGVO der primäre Rechtsrahmen behördlicher Verarbeitungen.[18]

Auch Verarbeitungen zum Zwecke der Gefahrenabwehr durch die zuständigen nationalen Behörden werden von den Regelungen der DSGVO nicht umfasst und von der JI-Richtlinie aufgegriffen.

Darunter fallen mithin auch Verarbeitungen, die der strafrechtlichen Prävention dienen, etwa verwaltungsbehördliche Überprüfungen der Eignungsfähigkeit für die Ausstellung eines Waffenscheins.[19]

[18] Wolff in BeckOK DatenschutzR, § 45 BDSG, Rn. 11; vgl. ErwG 19 DSGVO
[19] Wolff in BeckOK DatenschutzR, § 45 BDSG, Rn. 27

Bedingt durch den vorgesehenen Zweck kommt es also darauf an, ob die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Justizbehörden der DSGVO oder dem BDSG zu entnehmen ist.

D. Grundlagen

I. Ermittlungsverfahren

Beginn eines jeden Strafprozesses stellt die Einleitung des Ermittlungsverfahrens dar. Nach §152 Abs. 1 StPO gilt es für die Staatsanwaltschaft Ermittlungen einzuleiten, wenn sich nach Abs. 2 ein Anfangsverdacht gegenüber einer Person in einer Weise gebildet hat, dass die Annahme gerechtfertigt ist, dass eine Straftat begangen wurde, eine solche versucht wurde oder diese noch begangen werden soll. Dabei muss es sich um tatsächlich greifbare Annahmen handeln und nicht um eine Wahrscheinlichkeitsprognose, welche die Möglichkeit der Begehung einer Straftat aufgrund bestimmter Umstände berechnet oder auf rein kriminologischer Erfahrung beruht.[20] Bei den Annahmen muss es sich aber noch nicht um konkrete Beweise handeln, es muss lediglich die faktische Verwirklichung einer Straftat durch vorliegende Erkenntnisse als möglich erscheinen lassen, für deren Würdigung der Staatsanwaltschaft ein Spielraum zusteht.[21] Eins solche Annahme kann sich etwa aus dem Eingang einer Anzeige bei der Polizei ergeben. Gleichermaßen können Ermittlungen aber etwa auch aufgenommen werden, nachdem sich Hinweise auf das Vorliegen einer Straftat durch mediale Berichterstattung ergeben haben. Erhält die Staatsanwaltschaft Kenntnis vom Verdacht auf eine Straftat, so ist diese gem. §160 Abs. 1 StPO dazu verpflichtet das Ermittlungsverfahren zu eröffnen und den zugrundeliegenden Sachverhalt genauer zu erforschen. Diese Erforschung muss jedoch nicht zwangsläufig durch die

[20] Diemer in KK-StPO, §152 StPO Rn. 7
[21] BGH, Urteil v. 21.04.1988 - III ZR 255/86 (Celle); BVerfG, Urteil v. 08.11.1983 – 2 BvR 1138/83

Staatsanwaltschaft selbst erfolgen. Nach §161 Abs. 1 StPO kann die Sachverhaltsaufklärung nach Anweisung der Staatsanwaltschaft aber auch durch die Polizeibehörden erfolgen. §161 Abs. 1 S. 2 StPO verpflichtet dabei die Polizeibehörden, einer solchen Anweisung der Staatsanwaltschaft auch zu entsprechen. Eine solche Verpflichtung zum Tätigwerden trifft allerdings nicht nur die Staatsanwaltschaft selbst. Gem. §163 Abs. 1 StPO obliegt es auch den Polizeibehörden entsprechenden Hinweisen nachzugehen, insofern sie tatsächliche Kenntnis erlangen, nicht zuletzt deswegen, um einer etwaigen Verdunklung vorzubeugen. Dies geschieht nicht zuletzt in Verkehrskontrollsituationen, bei denen Beamte im Verlaufe der Kontrolle Anhaltspunkte dafür finden, dass eine Straftat verwirklicht sein könnte, etwa die Trunkenheit im Verkehr nach §316 Abs. 1 StGB. Die Polizei sammelt demnach alle Erkenntnisse und leitet sie im Anschluss an die Staatsanwaltschaft weiter. Zum Ermittlungsverfahren gehört neben der Beleuchtung des Sachverhaltes auch die Sicherung von Beweismaterial[22] und die Durchführung von Zeugenvernehmungen (§163 Abs. 3 StPO).[23] Wurde einem Betroffenen nach Vorliegen eines Anfangsverdachts i.S.v. §152 Abs. 2 StPO der Beschuldigtenstatus eröffnet, so ist dieser ebenfalls nach §163a Abs. 1 StPO zu vernehmen. Dabei ist es gem. §160 Abs. 2 StPO Aufgabe der Ermittlungsbehörden, in gleicher sorgfältiger Ermittlungsweise auch nach für den Beschuldigten entlastenden Hinweisen zu suchen.[24] Schlussendlich entscheidet auch die Staatsanwaltschaft ob nach Beendigung der Ermittlungen ein derart hinreichender Tatverdacht vorliegt, dass Anklage erhoben, ein Strafbefehl erstellt oder das Verfahren eingestellt wird. In der Realität kommt es im Rahmen der Ermittlungen allerdings regelmäßig zu einer Devianz von der gesetzlich vorgesehenen Regelung: eigenständige polizeilichen Untersuchungen, welche erst nach deren Abschluss an die Staatsanwaltschaft übermittelt werden, damit diese nur noch über eine mögliche Anklageerhebung zu entscheiden hat.[25] Von

[22] Kölbel in MüKo-StPO, §160 StPO Rn. 80
[23] Weingarten in KK-StPO, §163 StPO Rn. 15
[24] Kölbel in MüKo-StPO, §160 StPO Rn. 78
[25] Frister in Lisken/Denninger, PolR-HdB, Kapitel F. Rn. 16

einer Vertiefung der daraus resultierenden Problematik soll hier aber abgesehen werden.

II. Strafrecht und Ordnungswidrigkeiten

Umsetzungszweck der JI-RL ist nach deren Art. 1 der Erlass von Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung. Dabei stellt sich die Frage, inwieweit auch Verarbeitungen zum Zwecke der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Ordnungswidrigkeiten mit umfasst werden sollen.

Die grundsätzliche Charakterisierung eines Delikts als Straftat richtet sich danach, ob die Anwendungsmöglichkeit des Strafgesetzbuches gegeben ist, also die Ausführung einer dort geregelten tatbestandlichen Handlung oder deren Erfolg mit Geld- oder Freiheitsstrafe belegt ist.[26] Bei reinen Ordnungswidrigkeiten hingegen kommt zur Sanktionierung lediglich eine Geldbuße in Betracht.[27] Während also mit der Einstufung einer Handlung als Straftat vor allem der durch die Sanktion gewährleistete staatliche Schutz der allgemeinen Werteordnung gewährleistet wird,[28] so wird die Einstufung einer Handlung als Ordnungswidrigkeit und der Sanktionierung dieser als nachdrückliche staatliche Mahnung an bürgerliche Pflichten gesehen.[29] Der Begehung einer Ordnungswidrigkeit liegt somit demnach kein grundsätzliches kriminelles Unrecht zugrunde.[30]

Dennoch liegt sowohl dem Strafrecht als auch dem Ordnungswidrigkeitenrecht ein Sanktionierungsgedanke bestimmter Handlungen zugrunde.[31] Weiter besagt etwa §46 Abs. 1 OWiG die generelle Anwendung strafrechtlicher Gesetze und Verfahrensvorschriften für das sich aus dem Ordnungswidrigkeitenrecht

[26] Gerhold in BeckOK OWiG, Einleitung zum OWiG Rn. 2
[27] Unkroth in BeckOK PolR Bayern, Art. 1 LStVG Rn. 13
[28] BVerfG, Beschluss v. 16.07.1969 - 2 BvL 2/69
[29] Unkroth in BeckOK PolR Bayern, Art. 1 LStVG Rn. 13
[30] Unkroth in BeckOK PolR Bayern, Art. 1 LStVG Rn. 12
[31] Hornung, ZIS 2018, 566

ergebende Bußgeldverfahren. Die Verfolgungsbehörde erhält nach Abs. 2 dabei dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten. Unionsbegrifflich wird unter den Terminus der „Strafsache“ nach Art. 82 AEUV dabei auch gleichermaßen Verfahren aus dem Strafrecht und dem Ordnungswidrigkeitenrecht verstanden.[32] Auch die JI-RL greift die Begrifflichkeit auf und versteht die Anwendung ihrer Vorschriften auf eben diese.[33] Schließlich zählt auch die Rechtsprechung das deutsche Ordnungswidrigkeitenrecht als Teil des Strafrechtes.[34] So hat auch der deutsche Gesetzgeber in §46 BDSG explizit die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Ordnungswidrigkeiten explizit ergänzend in den Wortlaut mit aufgenommen. Eine Vertiefung des Streites kann an dieser Stelle also dahinstehen, die Vorschriften der §46 ff BDSG erstrecken sich damit auch auf Ordnungswidrigkeiten.

E. Grundsätze der Verarbeitung personenbezogener Daten

Um den Rechtsrahmen bei der Verarbeitung personenbezogener Daten durch die Polizei bei strafprozessualen Ermittlungen festzustellen, muss zunächst der Anwendungsbereich der einschlägigen Gesetze positiv festgestellt werden. Dabei wird ein Zweck der Verarbeitung, welcher zu Erkenntnissen im Rahmen des Ermittlungsverfahrens führt, angenommen.

I. Anwendungsbereich DSGVO

a) Sachlich

Nach Art. 2 Abs. 1 DSGVO gilt die Verordnung grundsätzlich für die Verarbeitung personenbezogener Daten, welche in einem Dateisystem

[32] Hornung, ZIS 2018, 566
[33] vgl. ErwG 7 JI-Richtlinie
[34] EGMR, 21.02.1984 - 8544/79;

gespeichert sind oder gespeichert werden sollen. Ein Dateisystem kennzeichnet sich nach Art. 4 Nr. 6 DSGVO hierbei maßgeblich durch strukturell gesammelte Daten, welche nach gleichartigen Kriterien zugänglich sind. Eine solche Gleichartigkeit hinsichtlich der zu beurteilenden Kriterien liegt bereits vor, wenn das Dateisystem Informationen nach einem Namen gliedert.[35] Der Datenträger des Dateisystems selbst muss dabei keine gespeicherten digitalen Daten enthalten, sondern kann auch in Papierform als solcher angesehen werden.[36] Vorliegend ist davon auszugehen, dass die von der Polizei bei der Ermittlungsarbeit erfassten oder zu erfassende Daten auch in einem Dateisystem gespeichert werden sollen. Dies ist allein schon deswegen anzunehmen, da eventuelle Erkenntnisse, welche aus den Daten des Betroffenen gewonnen werden, auch im Rahmen eines Strafprozesses verwendet werden sollen. Gleichermaßen kann etwa ein Datenabgleich nur vorgenommen werden, wenn die Daten bereits in einem Dateisystem gespeichert zur Verfügung stehen. §483 Abs. 1 S. 1 StPO stellt dabei die Erlaubnisnorm für die polizeiliche Speicherung in Dateisystemen zu strafprozessualen Zwecken dar. §483 Abs. 1 Nr. 1-3 StPO konkretisieren die Mindestanforderungen Informationssysteme nach Abs. 2, in welchen die Polizei ebenfalls Daten speichern darf, insofern eine gesetzliche Grundlage hierfür besteht.

Jedoch könnte eine Ausnahme nach Art. 2 Abs. 2 DSGVO einschlägig sein. Diese versagt die sachliche Eröffnung des Anwendungsbereiches der DSGVO, wenn Daten durch zuständige Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung verarbeitet werden. Vorliegend wird die Verarbeitung personenbezogener Daten durch polizeiliche Behörden im Rahmen strafprozessualer Maßnahmen betrachtet. Zu solchen Maßnahmen zählen insbesondere die aufgezählten Zwecke. Die Polizei ist als Behörde für die Verfolgung dieser Zwecke zuständig. Folglich ist die Ausnahme des Art. 2 Abs. 2 DSGVO einschlägig.

[35] Schild in BeckOK DatenschutzR, Art. 6 DSGVO, Rn. 83
[36] VG Gelsenkirchen, Urteil v. 27.04.2020 – 20 K 6392/18; LAG Sachsen-Anhalt, Urteil v. 23.11.2018 – 5 SA 7/17 (ArbG Magdeburg)

b) Zwischenergebnis

Der sachliche Anwendungsbereich der DSGVO ist nicht eröffnet.

II. Anwendungsbereich BDSG

a) Sachlich

Der Anwendungsbereich des BDSG muss nach Maßgabe des §1 BDSG eröffnet sein.[37] Nach §1 Abs. 1 ist der Anwendungsbereich für öffentliche Stellen des Bundes (1.) und öffentliche Stellen der Länder (2.), welche ihre Tätigkeiten aufgrund einer Organfunktion in der Rechtspflege wahrnehmen und reine Verwaltungsangelegenheiten ausgeschlossen sind, eröffnet.

Vorliegend werden polizeiliche Maßnahmen, die im Rahmen von Strafprozessen erfolgen, untersucht. Polizeiliche Maßnahmen werden in der Regel von Polizeibehörden ausgeführt,[38] welche sowohl als Bundes- als auch Landesbehörden auftreten können. Die Polizei selbst ist allerdings kein Organ der Rechtspflege, kann aber etwa im Rahmen der Übernahme von Ermittlungsarbeiten für die Staatsanwaltschaft für solche tätig werden.

Nachdem die Verarbeitung der personenbezogenen Daten durch Polizeibehörden zu Zwecken der Strafverfolgung erfolgt und somit nach Art. 2 Abs. 2 DSGVO die DSGVO nicht anwendbar ist, konkretisiert §45 BDSG den sachlichen Anwendungsbereich.[39] Diese Vorschrift erklärt in S. 1 die Anwendbarkeit des dritten Teils des BDSG für eben jene Zwecke, die von der DSGVO explizit ausgenommen sind und entsprechen damit auch genau den Zwecken, die vom Regelungsgehalt der JI-Richtlinie umfasst sind.

[37] Klar in Kühling/Buchner, DS-GVO BDSG, §1 BDSG, Rn. 2
[38] Ggf. können auch Beliehene polizeiliche Maßnahmen vornehmen: BGH, Urteil v. 21.01.1993 – III ZR 189/91 (Hamm)
[39] Klar in Kühling/Buchner, DS-GVO BDSG, § 1BDSG, Rn. 2

Die Verarbeitung muss dabei aber zwingend zur Erfüllung der in diesem Rahmen übertragenen Aufgaben erfolgen.

Vorliegend wird die Einwilligung betroffener Personen bei polizeilichen Ermittlungen aufgrund strafprozessualer Maßnahmen betrachtet. Zu strafprozessualen Maßnahmen zählen insbesondere auch zu führende Ermittlungen durch zuständige Behörden, welche auch explizit in §45 S.1 BDSG aufgeführt wird.

Der sachliche Anwendungsbereich des BDSG ist mithin eröffnet.

b) Räumlich

Um die Anwendbarkeit der Vorschriften des BDSG festzustellen, muss der räumliche Anwendungsbereich des BDSG ebenfalls eröffnet sein.

Nach §1 Abs. 4 S. 1 BDSG ist der räumliche Anwendungsbereich für öffentliche Stellen grundsätzlich eröffnet.[40] Davon erfasst sind gleichermaßen Zwecke für Verarbeitungen, welche aufgrund der in der DSGVO vorgesehenen Öffnungsklauseln vorgenommen werden, als auch solche Verarbeitungen, die gerade zu Zwecken der Straffverfolgung durchgeführt werden und aus der Umsetzung der JI-Richtlinie resultieren.[41]

Vorliegend werden polizeiliche Maßnahmen untersucht. Die Polizeibehörden können - wie oben festgestellt - öffentliche Stellen nach §2 Abs.1 BDSG sein, wenn sie als Bundesbehörden fungieren, nach §2 Abs. 2 BDSG, wenn sie als Landesbehörden Aufgaben des Bundes übernehmen oder für Organe der Rechtspflege Tätigkeiten ausführen. §45 BDSG S.1 konkretisiert erneut aber in jedem Falle die Anwendbarkeit auf öffentliche Stellen, welche zum Zwecke der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten und Ordnungswidrigkeiten personenbezogene Daten verarbeiten, unter welche die im vorliegenden Sachverhalt zu untersuchenden Verarbeitungen in jedem Fall zu fassen sind.

[40] Schmidt in Taeger/Gabel, DSGVO – BDSG – TTDSG, §1 BDSG Rn. 26
[41] Klar in Kühling/Buchner, DS-GVO BDSG, §1 BDSG Rn. 19

Der räumliche Anwendungsbereich des BDSG ist somit eröffnet.

c) Zwischenergebnis

Als Zwischenergebnis kann festgehalten werden, dass der Anwendungsbereich des BDSG eröffnet ist, da für den zugrundeliegenden Sachverhalt sowohl die sachlichen als auch räumlichen Voraussetzungen vorliegen.

III. Allgemeine Grundsätze

Nach Feststellung des zu berücksichtigenden Rechtsrahmens gilt es nun die genauen Voraussetzungen für die Verarbeitung personenbezogener Daten nach Maßgabe des BDSG zu analysieren.

Verarbeitungen zum Zwecke strafprozessualer Maßnahmen dürfen nur erfolgen, insofern die allgemeinen Grundsätze zur Verarbeitung personenbezogener Daten gewahrt sind. Nach §3 BDSG ist eine Verarbeitung personenbezogener Daten ausschließlich durch öffentliche Stellen grundsätzlich zulässig, wenn diese für die Erfüllung einer Aufgabe, die in der Zuständigkeit der verantwortlichen öffentlichen Stelle liegt oder dieser in Ausübung öffentlicher Gewalt übertragen wurden, notwendig ist. §1 Abs. 2 BDSG S. 1,2 erklärt die Vorschrift einer grundsätzlichen Subsidiarität unterliegend, insofern andere Rechtsvorschriften des Bundes, die den Datenschutz betreffen in Betracht kommen.[42]

Nach einer Auffassung kann eine solche Subsidiarität des §3 BDSG kann allerdings auch innerhalb der verschiedenen Teile des BDSG angenommen werden, insofern dort speziellere Vorschriften getroffen werden.[43]

Als bereichsspezifische Vorschrift und insofern als speziellere Norm vorgehend erscheinen hier vor allem §§47 ff. BDSG. Diese legen spezielle Grundsätze und Rechtsgrundlage für die Verarbeitung

[42] Starnecker in Gola/Heckmann, DS-GVO BDSG, §3 BDSG, Rn. 1
[43] Lang in Taeger/Gabel, DSGVO – BDSG – TTDSG, §3 BDSG, Rn. 14

personenbezogener Daten zu den in §45 BDSG genannten Zwecken fest. Da vorliegend §45 BDSG für anwendbar festgestellt wurde, würden insofern auch im Weiteren die §§47 ff. BDSG für die Untersuchung des Sachverhaltes gelten.

Nach anderer Auffassung bildet §3 BDSG gleichwohl des subsidiären Charakters der Norm, nicht nur eine Auffangnorm für öffentlich-rechtliche Datenverarbeitungen mangels spezialgesetzlicher Regelungen,[44] sondern auch eine allgemeine Grundlage für die Anwendung der in §45 BDSG geregelten Zwecke.[45] Demnach würden die Regelungen der §§47 ff. BDSG die Vorschrift des §3 BDSG konkretisieren für den Falle, dass §45 BDSG anwendbar ist.

Überzeugend erscheint hier die zweite Ansicht. Schon aufgrund der Tatsache, dass in Art. 8 der umzusetzenden JI-Richtlinie der Auftrag an den nationalen Gesetzgeber gestellt wird, eine Verarbeitung personenbezogener Daten zu den in der Richtlinie aufgeführten Zwecken nur als rechtmäßig anzuerkennen, insofern diese für die Erfüllung der Aufgabe einer zuständigen Behörde als erforderlich angesehen wird, soweit diese mit einer nationalen oder unionsrechtlichen Rechtsgrundlage ausgestattet ist. Der deutsche Gesetzgeber hat sich hier am Wortlaut des Art. 8 JI-RL orientiert und die Vorgaben in §3 BDSG überführt, während hingegen §45 BDSG gerade nicht die Vorgaben des Art. 8 JI-RL adressiert. Auch die Systematik der Normplatzierung innerhalb des ersten Teiles des BDSG, welcher gemeinsame Bestimmungen festlegt, lässt darauf schließen, dass innerhalb dieses Teiles genau diese Regelungen festgelegt werden sollen, welche in der Folge sich auf alle weiteren Teile des BDSG gleichermaßen erstrecken[46]. Eine Subsidiarität ist dementsprechend abzulehnen. Diese ergibt sich darüber hinaus auch nicht aus dem Wortlaut des §1 Abs. 2 BDSG, welcher die Subsidiarität gerade explizit für Vorschriften außerhalb des BDSG feststellt.

[44] Wolff in Beck OK Datenschutzrecht, §3 BDSG, Rn. 1
[45] Starnecker in Gola/Heckmann, DS-GVO BDSG, §3 BDSG, Rn. 2; Reimer in Sydow/Marsch, DS-GVO|BDSG, §3 BDSG, Rn. 3
[46] Wolff in Beck OK Datenschutzrecht, §3 BDSG, Rn. 1

In der Folge gelten sowohl die Bestimmungen des §3 BDSG als auch die Anforderungen der §§47 ff. BDSG für die Verarbeitung von personenbezogenen Daten im Kontext strafprozessualer Maßnahmen.

a) Personenbezogenes Datum

Um den allgemeinen Grundsätzen der Datenverarbeitung zu unterliegen, muss als Grundlage der Verarbeitung ein personenbezogenes Datum vorliegen.

Innerhalb des ersten Teils, der gemeinsamen Bestimmungen des BDSG, findet sich keine eigene Definition von personenbezogenen Daten.[47] Vielmehr wird die in Art. 4 Nr. 1 DSGVO angeführte Legaldefinition auch für das BDSG verwendet.[48] Diese ist jedenfalls insoweit anzuwenden, wenn Vorschriften im BDSG die in der DSGVO aufgeführten Regularien konkretisieren. Beispielhaft aufzuführen sind hier etwa Regelungen zum Beschäftigtendatenschutz nach Maßgabe des §26 BDSG, für welchen gem. Art. 88 Abs. 1 DSGVO durch die Mitgliedsstaaten nationale bereichsspezifische Vorschriften getroffen werden können.[49] Für den Bereich der Datenverarbeitung im Kontext strafprozessualer Maßnahmen wurde die DSGVO als nicht anwendbar festgestellt. Dementsprechend kann auch nicht direkt auf die in Art. 4 Nr. 1 DSGVO beschriebene Definition zurückgegriffen werden. Stattdessen wird die in § 46 Nr. 1 BDSG aufgeführte Legaldefinition für personenbezogene Daten herangezogen, die Art. 4 Nr. 1 DSGVO allerdings fast wortgleich ist und inhaltlich übereinstimmt.[50] Diese Definition entsprich dabei auch Art. 3 Nr. 1 JI-Richtlinie, deren Umsetzung Grundlage für den dritten Teil des BDSG ist.

Demnach sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

[47] Böken in Sydow/Marsch, DS-GVO|BDSG, §1 BDSG, Rn. 4
[48] Petri in Kühling/Buchner, DS-GVO BDSG, §3 BDSG, Rn. 5
[49] Riesenhuber in BeckOK DatenschutzR, §26 BDSG, Rn. 1
[50] Schulz in Gola/Heckmann, DS-GVO BDSG, §46 BDSG Rn. 5

(1) Vorliegen einer Information

Das Vorliegen einer Information ist dabei weit auszulegen[51] und umfasst grundsätzliche alle Arten, objektive wie subjektive[52] und auch Merkmale über Sachgegenstände, solange diese sich auf eine natürliche Person beziehen lassen.[53] Meinungen werden gleichermaßen wie Tatsachen erfasst, eine Information muss als keinen Wahrheitsgehalt aufweisen.[54]

Dies ist insbesondere insofern wichtig, als dass etwa im Rahmen strafrechtlicher Ermittlungen ein Beschuldigter keiner Pflicht unterliegt außerhalb seiner Personalien wahrheitsgemäße Angaben zum Sachverhalt zu machen. Die Äußerungen eines Beschuldigten zur Sache sind also in jedem Falle Informationen i.S.d. §46 Nr. 1 BDSG, unabhängig davon, ob diese zutreffend sind oder nicht. Auch die Erkenntnisse aus einem von der Polizei durchgeführten Alkohol- oder Drogentest, sind Informationen, die sich der Person des Getesteten zuschreiben lassen. Ebenfalls einen Personenbezug aufweisend sind Gutachten über Sachgegenstände eines Betroffenen.[55]

(2) natürlicher Personenbezug

Der Personenbezug ist außerdem nur bei natürlichen Personen gegeben. In der Konsequenz sind somit analog zum Anwendungsbereich der DSGVO auch im dritten Teil des BDSG explizit juristische Personen von der Begriffsdefinition ausgenommen.[56] Da eine juristische Person nach gegenwärtigem deutschen Recht – anders als in einigen anderen EU-Mitgliedsstaaten[57] – keiner Strafbarkeit unterliegen kann,[58] kann sie in der Folge auch nicht selbst unmittelbarer Täter sein.[59] Zwar kann ein

[51] Klar in Kühling/Buchner, DS-GVO BDSG, Art. 4 DSGVO Rn. 8
[52] EuGH (2. Kammer), Urteil v. 20.12.2017 – C-434/16
[53] Karg in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 25
[54] Ziebarth in Sydow/Marsch, DS-GVO | BDSG, Art. 4 DSGVO Rn. 41
[55] VG Schwerin Urteil v. 29.4.2021 – 1 A 1349/19 SN
[56] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 5
[57] Vgl. Übersicht zum Unternehmensstrafrecht in einzelnen Mitgliedsstaaten der Europäischen Union, WD 7 – 3000 – 070/17, https://www.bundestag.de/resource/blob/539400/9f7fe461015429dc5f71c4c3d2816704/wd-7-070-17-pdf-data.pdf; abgerufen am 25.06.2023
[58] Scholz, ZRP 2000, 435; Meyberg in BeckOK OWiG, §30 OWiG Rn. 1
[59] Meyberg in BeckOK OWiG, §30 OWiG Rn. 48

Unternehmen grundsätzlich durch das Ordnungswidrigkeitenrecht, etwa nach §30 OWiG durch Bußgelder sanktioniert werden, die dahinterstehende zu sanktionierende Handlung ist auch der juristischen Person zuzurechnen, muss aber gerade wieder zwingend durch eine natürliche Person begangen worden sein,[60] was auch eine Sanktionsverhängung gegen die natürliche Person möglich macht.[61] Ferner kann eine juristische Person auch Adressat strafprozessualer Maßnahmen sein, etwa aufgrund einer angeordneten Durchsuchung nach §103 Abs. 1 StPO.[62] Wird allerdings eine solche Maßnahme durchgeführt, so können Erkenntnisse daraus – positiv wie negativ – wiederum einer oder mehreren natürlichen Personen zugeordnet werden, etwa bei natürlichen Gesellschaftern oder Geschäftsführern und somit bei diesen ein personenbezogenes Datum begründen.[63]

(3) Identifizierbarkeit einer Person

Weiter unterscheidet der Wortlaut zwischen Informationen, durch welche eine Person bereits identifiziert ist und solchen, die eine Person potenziell identifizierbar machen. Eine unmittelbare Identifizierbarkeit einer natürlichen Person liegt dann vor, wenn von einer vorliegenden Information oder einem Datum direkt auf eine Person geschlossen werden kann. Eine solche unmittelbare Identifizierung einer Person lässt sich beispielsweise aus deren Namen ableiten.[64] Gleichermaßen können aber auch eindeutige zuordenbare Personenkennziffern i.S. des Art. 87 DSGVO, neben Pass- und Personalausweisnummern[65] etwa auch die Steueridentifikationsnummer[66] oder die Sozialversicherungsnummer[67] eine Person eindeutig identifizieren. Auch die Summer einer beliebigen

[60] Scholz, ZRP 2000, 437
[61] Meyberg in BeckOK OWiG, §30 OWiG Rn. 5
[62] Heinrich/Weingast in KK-StPO, §103 StPO Rn. 1
[63] Klabunde in Ehmann/Selmayr, DS-GVO, Art. 4 Rn. 14
[64] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 16
[65] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 17
[66] Ehmann, ZD 2021, 509
[67] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 16

Kombination von Merkmalen, welche eine natürliche Person betreffen, kann zu einer eindeutigen Identifizierbarkeit führen.[68]

Im Kontext der strafprozessualen Maßnahmen spielen vor allem die erwähnten Daten der Namen und Ausweisnummern eine tragende Rolle, da diese maßgeblich dazu dienen eine Person zu identifizieren.

Eine potenzielle Identifizierbarkeit einer natürlichen Person liegt vor, wenn die Information über eine bestimme Eigenschaft oder einer Tatsache einer Person zuordenbar oder zurechenbar gemacht werden kann und dies zur Folge hat, dass sie von anderen natürlichen Personen abgrenzbar ist.[69] Dies kann grundsätzlich jede Meinungsäußerung, Handlung, aber auch Informationen über Eigentums- oder Besitzverhältnisse sein, genauso wie individuelle Ausprägungen der eigenen körperlichen Beschaffenheit oder Informationen die Gesundheit oder die berufliche Ausprägung betreffend.[70] Dabei besteht keine spezielle Formgebundenheit der Informationen[71], diese können grundsätzlich in jedweder Form wie schriftlich, textlich oder elektronisch, aber auch verbalisiert vorliegen.[72] Entscheidend ist lediglich, dass sich die Information auch in einem Datum wiederspiegelt, welches auf einem Datenträger verkörpert ist, damit auch die Speicherung in einem Dateisystem möglich ist.[73]

Im Kontext der strafprozessualen Maßnahmen fällt hierrunter etwa das polizeiliche oder staatsanwaltliche dokumentierte Feststellen von oder Wissen über Tatsachen[74], welche sich wiederum auf eine natürliche Person beziehen, etwa das Verwirklichen oder Nichtverwirklichen eines Straftat- oder Ordnungswidrigkeitstatbestandes.[75] Ebenfalls der

[68] Karg, ZD 2014, 285
[69] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 17
[70] s. dazu auch Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, Drittes Element: „Eine bestimmte oder bestimmbare“ [natürliche Person], WP 136 01248/07/DE, https://www.lda.bayern.de/media/wp136_de.pdf; abgerufen am 29.06.2023
[71] EuGH, Urteil v. 10.7.2018 – C-25/17
[72] Arning in Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 4 DSGVO Rn. 7
[73] Ernst in Paal/Pauly, DS-GVO BDSG, Art. 4 Rn. 24, 25
[74] Klar in Kühling/Buchner, DS-GVO BDSG, Art. 4 DSGVO Rn. 26
[75] Müller in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 426

Identifizierbarkeit zuzuschreiben sind Aussagen einer Person, welche gegenüber Ermittlungsbeamten geäußert werden, etwa im Rahmen einer polizeilichen Aussage.[76] Auch im Rahmen einer Ermittlung anfallende KFZ-Kennzeichen[77] oder IP-Adressen[78] können potenziell eine Identifizierbarkeit gewährleisten oder diese begünstigen.

Ist die Identifizierbarkeit eines Datums nicht oder durch eine Anonymisierung nicht mehr möglich, so liegt kein Personenbezug vor und datenschutzrechtliche Vorschriften sind nicht unmittelbar auf die Verarbeitung dieses Datums anwendbar.[79]

(4) Zwischenergebnis

Ein personenbezogenes Datum kann demnach wie oben beschrieben im Rahmen strafprozessualer Maßnahmen durch polizeiliche Ermittlungen einfach begründet werden. Unschwer ist dies vor allem anzunehmen, wenn sich die Ermittlungen bereits gegen eine bekannte Person richten, da dann jedenfalls der Name der Person als personenbezogenes Datum anzusehen ist und auch die Anhaltspunkte, welche die Ermittlung begründen als personenbezogene Daten tauglich sind. Auch wenn sich Vorwürfe gegenüber einer Person im Rahmen der Ermittlung nicht aufrechterhalten oder sogar gänzlich widerlegen lassen, wird durch eine negative Feststellung[80] einer Tatsache ein personenbezogenes Datum begründet[81], da eine natürliche Person nun wiederrum von anderen Personen abgrenzbar ist oder individualisiert werden kann.[82]

b) Verarbeitung

Es muss weiter eine Verarbeitung des personenbezogenen Datums vorliegen.

[76] EuGH (2. Kammer), Urteil. v. 14.2.2019 – C-345/17
[77] OVG Münster, Urteil v. 19.10.2017 – 16 A 770/17
[78] OLG Frankfurt, Urteil v. 16.6.2010 – 13 U 105/07
[79] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 15
[80] vgl. ErwG 26 DSGVO
[81] Spindler in Spindler/Schuster, Recht der elektronischen Medien, Art. 4 DSGVO Rn. 5
[82] Karg in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 51

Eine Verarbeitung ist gem. §46 Nr. 2 BDSG jeder im Zusammenhang mit personenbezogenen Daten ausgeführte Vorgang der mit oder ohne Hilfe automatisierter Verfahren vorgenommen wird. Als Beispiele für eine mögliche Verarbeitung wird explizit das „Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, durch Übermittlung oder Verbreitung oder andere bereitgestellte Form offenlegen, Abgleichen, Verknüpfen, Einschränken, Löschen und Vernichten“ angeführt. Die Begriffsbestimmung der Verarbeitung des §46 Nr. 2 BDSG ist insofern wortgleich mit Art. 4 Nr. 2 DSGVO. Zur besseren Nachvollziehbarkeit der einzelnen Ausprägungen der Verarbeitungen im Kontext der Polizeiarbeit werden die aufgelisteten Varianten nachfolgend kurz skizziert.

(1) Verfahren der Verarbeitung

Da eine Verarbeitung gleichermaßen automatisiert wie manuell vorgenommen werden kann, ist der Rückschluss auf eine bestimmte verwendete Technik gerade nicht erforderlich.[83] Auch die Bestimmung oder Einordnung des Umfanges oder der Dauer der Verarbeitung ist für das zugrundeliegende Verfahren nicht von Bedeutung.[84] Im Kontext der strafprozessualen Maßnahmen kann also eine Abfrage oder ein Abgleich von Ausweisdaten einer natürlichen Person durch Polizeibeamte mittels technischer Kommunikation mit der Polizeibehörde[85] als auch die Vornahme einer Eingabe eines KFZ-Kennzeichens in eine behördliche Datenbank[86] unter den Begriff des Verfahrens einer Verarbeitung i.S. des §46 Nr. 2 BDSG fallen. Gleichermaßen ist auch das Anfertigen eines Vernehmungsprotokolls anzusehen, welches entweder computergestützt[87] aber auch händisch erfolgen kann.[88]

[83] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 33
[84] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 11
[85] Greven in KK-StPO, §98 StPO Rn. 20
[86] Greven in KK-StPO, §98 StPO Rn. 17
[87] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 34
[88] VG Gelsenkirchen – Urteil v. 27.4.2020 – 20 K 6392/18

(1) Erheben von Daten

Das Erheben von Daten beschreibt den Vorgang der Beschaffung von Daten über eine natürliche Person beim Betroffenen selbst.[89] Vorliegend kommt dies etwa in Betracht wenn Polizeibeamte etwa eine Person im Ramen ihrer Ermittlungen befragen und der Befragte antwortet.[90]

(2) Erfassen von Daten

Das Erfassen von Daten bezieht sich auf die Verkörperung personenbezogener Daten auf Datenträgern. Eine Erfassung liegt beispielsweise vor, wenn ein Polizeibeamter eine Lichtbildaufnahme einer Person anfertigt.[91] Aber auch das Anfertigen handschriftlicher Notizen, welche später den Ermittlungsakten beigefügt werden, gilt als Datenerfassung.[92]

(3) Organisieren von Daten

Die Organisation von Daten bezeichnet eine systematisch-strukturelle Anordnung von Daten[93], die daraufhin abzielt, eine weitere Verwendung der Daten einfach zu gestalten, etwa hinsichtlich deren Auffindbarkeit.[94] Im Kontext der polizeilichen Ermittlungen kann hierunter etwa die Zuordnung der erhobenen Daten in einzelne Kategorien innerhalb eines Dateisystems fallen, etwa Vorname, Nachname, Geburtsdatum, Adresse mit entsprechender Anlage als Datenbankfelder.[95]

(4) Ordnen von Daten

Das Ordnen von Daten knüpft direkt an die Organisation der Daten an[96] und beschreibt etwa eine chronologische Strukturierung der Daten

[89] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 35
[90] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 35
[91] Reimer in Sydow/Marsch, DS-GVO | BDSG, Art. 4 DSGVO Rn. 56
[92] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 16
[93] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 17
[94] Herbst in Kühling/Buchner, DS-GVO BDSG, Art. 4 DSGVO Rn. 23
[95] Hermes in Wandtke/Bullinger, UrhR, §87a UrhG Rn. 38
[96] Schild in BeckOK DatenschutzR, Art. 4 DSGVO, Rn. 43

innerhalb einer der Datenorganisation zugrundeliegenden Kategorien.[97] Ein Beispiel im vorliegenden Kontext könnte etwa die Zusammenstellung einer alphabetisch geordneten Liste aller Nachnamen innerhalb einer Suchanfrage innerhalb einer behördlichen Datenbank sein.[98]

(5) Speichern von Daten

Die Speicherung von Daten beschreibt die Verkörperung von Daten auf einem Datenträger,[99] wodurch diese der Aufbewahrung zugeführt werden sollen.[100] Insofern ist auch eine längerfristige Ablage der Daten ohne weitere Verarbeitung von der Begrifflichkeit der Speicherung umfasst,[101] da es gerade auf die Dauer der Speicherung nicht ankommt.[102] Im Rahmen der polizeilichen Ermittlung ist schon jede Anlage eines Datensatzes oder die Eingabe erfasster Daten, genau wie die Ablage eines Protokolls eine Speicherung i.S. des §46 Nr. 2 BDSG.

(6) Anpassen oder Verändern von Daten

Die Veränderung von Daten beschreibt jedwede am Datum selbst vorgenommene inhaltliche Änderung, welche sich anschließend auf den Informationsgehalt des Datums auswirkt.[103] Einer rein redaktionelle Korrektur eines Datums ist dagegen keine Veränderung.[104] Die Anpassung konkretisiert die Veränderung und beschreibt etwa die Aktualisierung eines Datums auf einen neuen Stand zu einem neuen Zeitpunkt.[105] Eine Anpassung im Rahmen der Polizeiarbeit stellt etwa die Überschreibung des Wohnortes in einer behördlichen Datenbank dar, wenn bei einer Person ein solcher Wohnortwechsel festgestellt wurde.

[97] Herbst in Kühling/Buchner, DS-GVO BDSG, Art. 4 DSGVO Rn. 23
[98] Reimer in Sydow/Marsch, DS-GVO | BDSG, Art. 4 DSGVO Rn. 60
[99] Herbst in Kühling/Buchner, DS-GVO BDSG, Art. 4 DSGVO Rn. 24
[100] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 19
[101] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 42a
[102] BGH, Beschluss v. 3.2.2011 – I ZR 129/08; Müller in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 436
[103] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 20
[104] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 45
[105] Herbst in Kühling/Buchner, DS-GVO BDSG, Art, 4 DSGVO Rn. 26

(7) Auslesen und Abfragen von Daten

Unter dem Auslesen von Daten ist der Zugriff auf gespeicherte Daten zu verstehen,[106] welche sich bereits im Verantwortungsbereich des für die Datenverarbeitung Verantwortlichen befindet,[107] etwa der Abruf eines Datensatzes aus der polizeieigenen Datenbank.[108] Das Abfragen von Daten erweitert das Auslesen auch auf externe Datenbanken[109] unter Zuhilfenahme einer technischen Suchroutine,[110] etwa eine Abfrage eines Kennzeichens in der Datenbank der KFZ-Zulassungsstelle.

(8) Verwenden von Daten

Die Verwendung von Daten i.S. des §46 Nr. 2 BDSG darf als Auffangtatbestand verstanden werden, um jene für bestimmte Zwecke[111] herangezogene Verarbeitungen abzudecken, welche nicht direkt unter die Aufzählungen in der Vorschrift subsumierbar sind.[112]

(9) Offenlegung von Daten

Die Offenlegung von Daten beschreibt die Zugänglichmachung bestimmter Daten für einen Nutzerkreis, der nicht der ursprüngliche Adressat der Daten war, bis hin zu einem Publikmachen für die Öffentlichkeit.[113] Ist der Nutzerkreis dem Offenlegenden bekannt, so werden die Daten übermittelt, bspw. durch Versand an einen Mailverteiler.[114] Ist die Personengruppe jedoch nicht bestimmbar, so tritt die Verbreitung an die Stelle der Übermittlung, etwa durch einen Blogpost.[115] Auf den Kommunikationskanal kommt es jedoch gerade nicht an.[116] Im Kontext der Betrachtung polizeilicher Arbeiten kann etwa

[106] Herbst in Kühling/Buchner, DS-GVO BDSG, Art. 4 DSGVO Rn. 27
[107] Reimer in Sydow/Marsch, DS-GVO | BDSG, Art. 4 DSGVO Rn. 63
[108] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 47
[109] Ernst in Paal/Pauly, DS-GVO BDSG, Art. 4 DSGVO Rn. 28
[110] Ernst in Paal/Pauly, DS-GVO BDSG, Art. 4 DSGVO Rn. 28; Herbst in Kühling/Buchner, DS-GVO BDSG, Art. 4 DSGVO Rn. 27
[111] Herbst in Kühling/Buchner, DS-GVO BDSG, Art. 4 DSGVO Rn. 28
[112] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 48
[113] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 49
[114] Reimer in Sydow/Marsch, DS-GVO | BDSG, Art. 4 DSGVO Rn. 69
[115] Reimer in Sydow/Marsch, DS-GVO | BDSG, Art. 4 DSGVO Rn. 69
[116] Ernst in Paal/Pauly, DS-GVO BDSG, Art. 4 DSGVO, Rn. 30

die Offenlegung eines Namens und Lichtbildes einer Person zu Fahndungszwecken, etwa in einer Fernsehsendung zählen.

(10) Abgleich und Verknüpfung von Daten

Der Abgleich von personenbezogenen Daten setzt voraus, dass bereits zwei unterschiedliche Datensätze bestehen, welche sich auf dieselben Kriterien einer natürlichen Person beziehen.[117] Durch den Abgleich wird meist ein neuerer Datensatz mit einem älteren verglichen und kann so auf eine Aktualisierung hinwirken, insofern Inkonsistenzen festgestellt wurden.[118] Als Beispiel des Abgleichs personenbezogener Daten im polizeilichen Kontext kann hierfür die Rasterfahndung genannt werden.[119]

Die Verknüpfung von personenbezogenen Daten beschreibt die Zusammenführung verschiedener Daten, die sich auf eine natürliche Person beziehen zu einem neuen Datensatz,[120] welcher für sich gesehen über einen höheren Informationsgehalt auf die bezugnehmende Person verfügt.[121] Gleichermaßen kann aber auch eine Verknüpfung mehrerer natürlicher Personen zu einer Information –aus polizeilicher Sicht etwa die Feststellung, dass mehrere natürliche Personen an einer Straftat beteiligt sind – eine Verknüpfung darstellen.[122]

(11) Einschränkung von Daten

Die Einschränkung personenbezogener Daten wird in §46 Nr. 3 BDSG als die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung zu verhindern, legaldefiniert. Es besteht insofern Wortgleichheit mit der Legaldefinition in Art. 4 Nr. 3 DSGVO. Eine Einschränkung kann gem. §58 Abs. 3 BDSG vorgenommen werden, wenn schutzwürdige Interessen einer betroffenen Person dies rechtfertigen (Nr. 1) bspw. bei einem andauernden

[117] Reimer in Sydow/Marsch, DS-GVO | BDSG, Art. 4 DSGVO Rn. 72
[118] Ernst in Paal/Pauly, DS-GVO BDSG, Art. 4 DSGVO, Rn. 31
[119] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 27
[120] Schild in BeckOK DatenschutzR, Art. 4 DSGVO Rn. 52
[121] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 28
[122] Ernst in Paal/Pauly, DS-GVO BDSG, Art. 4 DSGVO, Rn. 32

Auskunftsverlangen,[123] Daten zu Beweiszwecken im Rahmen von laufenden Gerichtsverfahren[124] weiter gespeichert werden müssen (Nr. 2) oder eine Löschung nur mit unverhältnismäßigem Aufwand möglich ist (Nr. 3). Die Ausnahme nach Nr. 3 ist in jedem Falle restriktiv zu verstehen[125] und kritisch zu betrachten, da diese nach Literaturstimmen[126] und DSK[127] nicht mit dem Unionsrecht vereinbar ist, da der Umsetzungsspielraum des Art. 16 JI-Richtlinie überschritten wurde. Nach §161 Abs. 2 StPO findet §58 Abs. 3 BDSG allerdinge keine Anwendung, soweit nach Maßgabe der StPO eine ausdrückliche Löschung vorzunehmen ist.

§489 StPO Abs. 6 erklärt in der Folge allerdings wiederum den §58 Abs. 3 Nr. 1, Nr. 3 BDSG i.S. einer Einschränkung für anwendbar und ergänzt weiterhin die Einschränkungsvornahme für eine weitere notwendige Forschungsbearbeitung (S. 2), bei ausschließlicher Speicherung zu Zwecken der Datensicherung oder Datenschutzkontrolle (S. 3) oder bei Vorliegen einer Beweisnot, zu derer Behebung die Verarbeitung unerlässlich ist (S. 5). Eine Unerlässlichkeit kann allerdings nur angenommen werden, wenn eine objektive Unmöglichkeit der anderweitigen Beweiserbringung vorliegt.[128] §489 Abs. 6 S. 4 StPO stellt klar, dass nach S. 1 oder S. 2 eingeschränkte Daten nur für die ursprünglich erhobenen Zwecke weiter gespeichert werden, insofern für diese die Löschung unterblieben ist.

Die §58 Abs. 3 Nr. 2 BDSG aufgeführte Erlaubnis zur lediglichen Einschränkung von Daten und die damit verbundene bewusste Nichtvornahme der Löschung ist insofern in Bezug auf den Strafprozess nur relevant, wenn eine Löschung nach StPO nicht explizit vorzunehmen ist.

[123] Nolte in Gola/Heckmann, DS-GVO BDSG, §58 BDSG Rn. 15
[124] Paal in Paal/Pauly, DS-GVO BDSG, §58 BDSG Rn. 10
[125] Paal in Paal/Pauly, DS-GVO BDSG, §58 BDSG, Rn. 11
[126] Schwichtenberg in Kühling/Buchner, DS-GVO BDSG Rn. 7; Otto in Sydow/Marsch DS-GVO | BDSG, §58 BDSG Rn. 27
[127] Stellungnahme der DSK zur Evaluierung des BDSG, 2.3.2031, S.32, https://www.datenschutzkonferenz-online.de/media/st/20210316_DSK_evaluierung_BDSG.pdf; abgerufen am: 6.7.2023
[128] Wittig in BeckOK StPO, §489 StPO Rn. 9

Die Markierung der zu sperrenden Daten muss dabei für alle Nutzer gleichermaßen unmissverständlich kenntlich machen, dass die zugrundeliegenden Daten für eine weitere Verarbeitung nicht herangezogen werden dürfen.[129]

(12) Löschen und Vernichten von Daten

Das Löschen eines Datums bezeichnet dessen komplette logische Entfernung von einem Datenträger, während der Datenträger als solcher erhalten bleibt.[130] Die Löschung eines Datums muss insoweit erfolgen, als dass das Wiederherstellen dieses Datums nicht oder nur mit einem größeren Aufwand möglich ist. Ein simples Löschen von der Festplatte stellt noch keine vollwertige Löschung dar, erst eine mehrfache Überschreibung der Platte nach Stand der Technik[131] stellt sicher, dass die Daten nicht mehr wiederhergestellt werden können.[132]

Beim Vernichten wird der Datenträger mit samt der auf ihm befindlichen Daten physisch zerstört.[133] Als Datenträger zählen hierbei nicht nur mechanische Festplatten (HDD)[134] und Flash-Speicher wie SSD,[135] sondern auch Papier[136] oder etwa ein Trägermedium die Rückschlüsse auf Analyseergebnisse von genetischem Testmaterial erlauben,[137] nicht aber etwa rein biologische Proben des Genmaterials selbst,[138] insbesondere wenn keine Analyse des Materials vorgesehen ist.[139]

---

[129] Dix in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 2; vgl. ErwG 67 DSGVO
[130] Reimer in Sydow/Marsch, DS-GVO | BDSG, Art. 4 DSGVO Rn. 75
[131] s. hierzu etwa Empfehlungen zum sichern Löschen des BSI: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html; abgerufen am 6.7.2023
[132] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 DSGVO Rn. 30
[133] Ernst in Paal/Pauly, DS-GVO BDSG, Art. 4 DSGVO Rn. 34
[134] z. Funktionsweise Schmidt in Auer-Reinsdorff/Conrad, IT-R-HdB, §2 Rn. 246-255
[135] z. Funktionsweise Schmidt in Auer-Reinsdorff/Conrad, IT-R-HdB, §2 Rn. 261-269; Scheja in Forgó/Helfrich/Schneider, Betr. Datenschutz, Kapitel 1: Datenschutzkonzepte Rn. 87
[136] Föhlisch in Hoeren/Sieber/Holznagel, MMR-HdB, Teil 13.4 Verbraucherschutz im Internet, Rn. 248
[137] Weichert in Kühling/Buchner, DS-GVO BDSG, Art. 4 Nr. 13 DSGVO Rn. 10
[138] Taupitz, MedR 2021, 413
[139] Weichert in Kühling/Buchner, DS-GVO BDSG, Art. 4 Nr. 13 DSGVO Rn. 10

(13) Zwischenergebnis

Es wurden für die in §46 Nr. 2 BDSG aufgezählten möglichen Verarbeitungen jeweils auch Beispiele der polizeilichen Arbeit aufgezeigt. Da die Grundlage der Untersuchung keine spezielle polizeiliche Ermittlungsausführung, sondern die Ermittlungen zu strafprozessualen Zwecken allgemein bildet, kann insofern davon ausgegangen werden, dass eine Verarbeitung i.S.d. §46 Nr. 2 BDSG vorliegt. Eine genaue Betrachtung ist dennoch sinnvoll, da die jeweilige Verarbeitung entsprechend kategorisiert werden kann und sich je nach Verarbeitungsart zusätzliche Anforderungen ergeben können.

c) Verarbeitung auf rechtmäßige Weise

Die Verarbeitung muss gem. §47 Nr. 1 BDSG auf rechtmäßige Weise stattfinden.

Auf rechtmäßige Weise wird eine Verarbeitung durchgeführt, wenn dieser eine Rechtsgrundlage zugrunde liegt. Eine im parlamentarisch durchgeführten Rechtserlassungsverfahren erlassene Vorschrift ist hierfür nach ErwG 33 der JI-RL gerade nicht zwingend, lässt aber national geltende Vorschriften unberührt. Für eine wirksame Rechtsgrundlage ist in Deutschland daher der Vorbehalt des Gesetzes zu berücksichtigen.[140] Der Vorbehalt des Gesetzes besagt, dass ein Eingriff in die Rechte, die ein Bürger vom Staat zugesichert bekommt, immer auf einem formell erlassenen Gesetz oder einer anderen auf diesem erlassenen Gesetz fußenden Rechtsnorm, beruhen müssen.[141] Dieser Grundsatz folgt unmittelbar aus dem verfassungsmäßig garantieren Rechtsstaats- und Demokratieprinzip aus Art. 20 GG.[142] Da eine Verarbeitung personenbezogener Daten auch immer einen Eingriff in das Recht auf informationelle Selbstbestimmung[143] aus Art. 2 Abs. 2 GG i.V.m. Art. 1

[140] Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 6
[141] Weber, Rechts-WB, Gesetzmäßigkeit der Verwaltung
[142] Rux in BeckOK GG, Art. 20 GG Rn. 173
[143] Das Recht eines jeden, den Umgang mit dem ihn betreffenden personenbezogenen Daten grundsätzlich selbst zu bestimmen; vgl. BVerfG, Urteil v. 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83

Abs. 1 GG darstellt,[144] bedarf es eines parlamentarisch erlassenen Rechtsaktes, welcher die Grundlage eines solchen Eingriffs darstellt.[145]

Vorliegend soll im Kontext der strafprozessualen Maßnahmen die Einwilligung als taugliche Rechtsgrundlage untersucht werden.

Die Einwilligung in die Verarbeitung eigener personenbezogener Daten durch staatliche Stellen stellt grundsätzlich einen Verzicht auf die Inanspruchnahme des vom Staat garantierten Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art.1 Abs. 1 GG, bzw. des Rechts auf Datenschutz aus Art. 8 GRCh dar.

Eine solche Grundrechtsdisposition ist unter Berücksichtigung der jeweils zutreffenden Umstände - nebst Verzichtserklärung das Vorliegen von Dispositionsbefugnis und Freiwilligkeit - grundsätzlich möglich.[146]

(1) Verzichtserklärung

Die Erklärung zum Verzicht auf die Inanspruchnahme eines Grundrechts kann sowohl ausdrücklich als auch konkludent erfolgen.[147] Wird ein Betroffener von den Polizeibehörden also nach seiner Einwilligung in eine strafprozessuale Maßnahme befragt, so kann diese gegenüber der Behörde zum Zeitpunkt des Ersuchens entweder durch verbale Zustimmung, etwa durch Bejahen, als auch durch nonverbale Zustimmung, etwa ein Nicken, erteilt werden. Gleichermaßen ist die Ablehnung durch Verneinen oder Kopfschütteln zu betrachten.

[144] BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83; Sobotta in Grabitz/Hilf/Nettesheim, Das Recht der EU, Art. 16 AEUV Rn. 7; Schild in NK-AuslR, §86 AufenthG Rn. 1
[145] Di Fabio in Dürig/Herzog/Scholz, GG, Art. 2 Abs. 1 GG Rn. 38
[146] ausführlich dazu: Fischinger, JuS 2007, 808
[147] Sachs in Sachs, GG, Vorbemerkung z. Abschnitt I Rn. 55

(2) Freiwilligkeit

Der Betroffene muss die Verzichtserklärung freiwillig abgeben. Von der Beurteilung der Freiwilligkeit auf den Verzicht auf ein Grundrecht abzugrenzen ist die Freiwilligkeit in die Einwilligung einer konkreten Datenverarbeitung. Vorliegend soll zunächst nur die Möglichkeit beleuchtet zu werden, einen Grundrechtsverzicht freiwillig zu erklären. Die Freiwilligkeit bei der Einwilligung in eine konkrete Datenverarbeitung wird im weiteren Verlauf problematisiert. Die Freiwilligkeit beim Verzicht auf Grundrechte kann angenommen werden, wenn der Verzichtende hinsichtlich seiner Erklärung nicht getäuscht oder diese durch eine Drucksituation herbeigeführt oder gänzlich erzwungen wurde.[148] Nicht freiwillig wäre eine Einwilligung auf den Verzicht der Grundrechte demnach, wenn dem Betroffenen seitens der Polizeibehörden mit strafrechtlichen Konsequenzen gedroht oder sogar dessen körperliche Unversehrtheit bedroht würde. Genauso ist die Sachlage zu beurteilen, wenn die Behörde die wahre Absicht der Maßnahme verschleiert oder bewusst falsche Hintergründe gegenüber dem Betroffenen angibt.

(3) Dispositionsbefugnis

Die betroffene Person muss außerdem befugt sein über den Verzicht ihrer Grundrechte zu disponieren. Eine solche Dispositionsbefugnis kann von Grundrecht zu Grundrecht variieren.[149] So wird etwa Art. 6 Abs. 2 GG, das Recht der Eltern auf Pflege und Erziehung ihrer Kinder gleichermaßen als Pflicht verstanden und ist daher kein Dispositionsgut.[150] Weiter wird eine Dispositionsbefugnis über die in Art. 1 Abs. 1 S. 1 GG verankerte Menschenwürde abgesprochen,[151] da diese als absolutes Schutzgut gilt[152] und auch schon der Wortlaut die

[148] Jarass in Jarass/Pieroth, GG, Vorbemerkungen vor Art. 1 GG Rn. 36; Voßkuhle, JuS 2009, 314
[149] Jarass in Jarass/Pieroth, GG, Vorbemerkungen vor Art. 1 GG, Rn. 35
[150] BVerfG, Beschluss v. 9.4.2033 – 1 BvR 1493/96; BVerfG, Beschluss v. 29.7.1968 – 1 BvL 20/63, 31/66 u. 5/67
[151] VG Neustadt, Beschluss v 21.5.1992 – 7 L 1271/92
[152] BVerfG, Urteil v. 21.6.1977 – 1 BvL 14/76

Unantastbarkeit darlegt. Gleichermaßen sind auch staatliche Eingriffe in die Menschenwürde untersagt.[153]

Dementsprechend kann ein Betroffener also auch keine Einwilligung gegenüber staatliche Behörden erbringen, wenn diese ihm eine Maßnahme anbieten, welche dessen Würde beschädigen würde, da selbst wenn eine Dipositionsbefugnis des Grundrechts angenommen würde, die Behörden den Eingriff durch die gewählte Maßnahme nicht durchführen dürfen.[154] Denkbar ist aber etwa ein Verzicht auf das Recht der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG, wenn der Grundrechtsberechtigte einer Durchsuchung seiner Wohnräumlichkeiten zustimmt.[155] Ähnliches gilt zunächst auch für die Durchsuchung seines Kraftfahrzeugs,[156] was den reinen Grundrechtsverzicht betrifft. Freilich gilt es die Dispositionsbefugnis im Einzelfall festzustellen, da in jedem Fall die angebotene Maßnahme und das betroffene Grundrecht in Abwägung stehen.[157]

(4) Zwischenergebnis

Grundsätzlich kann eine natürliche Person einen Verzicht auf ihre verfassungsrechtlich gewährten Grundrechte verzichten, wenn diese die Dispositionsbefugnis über das jeweilige Grundrecht innehat, in den Verzicht einwilligt und dies auch gegenüber der staatlichen Stelle erklärt hat. Mithin überzeugt es, dass es Teil der informationellen Selbstbestimmung ist, gerade diese Selbstbestimmtheit dahingehend walten zu lassen, dass ein Betroffener einwilligt Informationen über ihn an staatliche Stellen herauszugeben, bzw. diese durch Behörden verarbeiten zu lassen[158], wissentlich dass diese Verarbeitung durch die Behörden im weiteren datenschutzrechtlich normiert und beschränkt

[153] BVerfG, Beschluss v. 4.4.2006 – 1 BvR 518/02
[154] vgl. BGH, Urteil v. 22.12.2011 – 2 StR 509/10
[155] Jarass in Jarass/Pieroth, GG, Vorbemerkungen vor Art. 13 GG Rn. 10
[156] LG Kiel, Beschluss v. 19.8.2021 – 10 Qs 43/21
[157] Fischinger, JuS 2007, 811
[158] Albers in BeckOK DatenschutzR, Art. 6 DSGVO Rn. 29

ist.[159] Im weiteren wird auch deutlich, dass durch die Konstitution der Einwilligung als Rechtsgrundlage in §51 BDSG[160] der Gesetzgeber einen solchen Verzicht auf das betroffene Grundrecht ausdrücklich möglich machen wollte.[161] Das BDSG, welches die Rechtsgrundlage der Einwilligung anführt, wurde außerdem erforderlicherweise im parlamentarischen Akt, durch Zustimmung von Bundestag[162] und Bundesrat[163] rechtmäßig erlassen.[164]

d) Verarbeitung nach Treu und Glauben

Die Verarbeitung personenbezogener Daten muss nach §47 Nr. 1 BDSG auch nach Treu und Glauben stattfinden.

Der Grundsatz von Treu und Glauben ist im Kontext des Datenschutzrechtes vom dem im deutschen Zivilrecht schon lange verankerten gleichlautenden Grundsatz losgelöst zu betrachten.[165] Im Datenschutzrecht verspricht der Grundsatz, die in jedem Fall stattfindende Berücksichtigung der Interessen derjenigen Person, deren Daten einer Verarbeitung zugeführt werden sollen.[166] Diese sollen in vernünftiger Weise angenommen werden und bei der Abwägung der Durchführung herangezogen werden.[167] Weiter soll einer betroffenen Person alle notwendigen Angaben über mögliche aus der Verarbeitung resultierenden Risiken dargelegt werden, genau wie Informationen über in Zusammenhang stehende Vorschriften, Garantien und Rechte.[168] Dazu

[159] Masing, NJW 2012, 2305; s. Engeler, NJW 2022, 3398 zum Konflikt zwischen dem Recht auf Datenschutz aus Art. 8 GRCh und dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.
[160] vgl. Art. 6 Abs. 1 lit. a) DSGVO; ErwG 37 JI-RL
[161] Heckmann in Gola/Heckmann, DS-GVO – BDSG, §51 BDSG Rn. 2
[162] Plenarprotokoll zum Beschluss im Bundestag: https://dserver.bundestag.de/btp/18/18216.pdf; abgerufen am 16.07.2023
[163] Beschluss des Bundesrates: http://www.bundesrat.de/SharedDocs/drucksachen/2017/0301-0400/332-17(B).pdf?__blob=publicationFile&v=1; abgerufen am 16.07.2023
[164] Veröffentlichung des DSAnpUG-EU, welches die Änderungen im BDSG regelt: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1689521395666; abgerufen am 16.07.2023
[165] Herbst in Kühling/Buchner, DS-GVO BDSG, Art. 5 DSGVO Rn. 13
[166] Schantz in BeckOK DatenschutzR, Art. 5 DSGVO Rn. 8
[167] Heberlein in Ehmann/Selmayr, DS-GVO, Art. 5 DSGVO Rn. 10
[168] vgl. ErwG 26 JI-RL

zählt ebenfalls die Anzeige einer möglichen behördlichen Weitergabe der personenbezogenen Daten gegenüber der betroffenen Person.[169]

Weiter verstößt eine Verarbeitung gegen Treu und Glauben, wenn diese gemeinhin als sittenwidrig anzusehen ist.[170] Ein wesentlicher Unterschied bei der datenschutzrechtlichen Auslegung des Grundsatzes besteht aber auch innerhalb der einschlägigen Normen. Wird bei einer DSGVO-konformen Auslegung mithin auch ein Verbot der heimlichen Verarbeitung von personenbezogenen Daten unter der Befolgung von Treu und Glauben verstanden,[171] so fehlt es bei der Auslegung im Sinne des BDSG genau an dieser Anforderung. Hintergrund ist der im BDSG nicht konstituierte Transparenzgrundsatz bei der Datenverarbeitung. Im Gegensatz zu einer Verarbeitung nach außerhalb strafprozessualer Maßnahmen und nach Maßgabe der DSGVO muss es Ermittlungsbehörde gerade möglich sein, ihre Ermittlungen auch ohne Wissen oder Wollen einer natürlichen Person auszuführen,[172] um den Ermittlungserfolg nicht zu gefährden oder überhaupt erst herbeizuführen, etwa die durch die DSGVO in der Regel ausgeschlossene verborgene Überwachung von Personen in Bild und Ton.[173] Folgerichtig schließt die dem BDSG zugrundeliegende JI-Richtlinie solche verdeckten Datenverarbeitungen auch explizit ein.[174] Dies gilt zumindest zum Zeitpunkt der Vornahme der verdeckten Verarbeitung. Ist die Ermittlung abgeschlossen und werden Informationen aus der Verarbeitung nicht weiter benötigt, so ist die Mitteilung über die Datenverarbeitung gegenüber dem Betroffenen im Nachgang zu erbringen.[175]

Eine Verarbeitung zu strafprozessualen Maßnahmen dürfte aufgrund der engen Bindung der ermittelnden Behörden an die zugrundeliegenden Gesetze und der damit verbundenen Rechtsgrundlage regelmäßig dem Grundsatz von Treu und Glauben entsprechen,[176] insofern die Behörden

[169] EuGH (Dritte Kammer), Urteil v. 01.10.2015 – C-201/14
[170] Reimer in Sydow/Marsch, DS-GVO | BDSG, Art. 5 DSGVO Rn. 14
[171] Herbst in Kühling/Buchner, DS-GVO BDSG, Art. 5 DSGVO Rn. 15
[172] Johannes in Sydow/Marsch, DS-GVO | BDSG, §47 BDSG Rn. 22
[173] Pötters in Gola/Heckmann, DS-GVO BDSG, Art. 5 DSGVO Rn. 10
[174] Braun in Gola/Heckmann, DS-GVO BDSG, §47 BDSG Rn. 12
[175] vgl. ErwG 26 JI-RL; Johannes in Sydow/Marsch DS-GVO | BDSG Rn. 22
[176] Müller in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 595

für die zugrundeliegende Maßnahme auch objektiv genug Anhaltspunkte vorliegen haben, um eine Datenverarbeitung im Rahmen der Ermittlungen zu begründen, was die enge Bindung des Grundsatzes von Treu und Glauben zum Grundsatz der Rechtmäßigkeit nochmalig unterstreicht. Diese Voraussetzungen sind auch bei der Einwilligung eines Betroffenen anzusetzen. Gibt es für die Behörde Grund zur Annahme, dass durch eine Einwilligung eines Betroffenen für die Ermittlung wichtige Erkenntnisse gewonnen werden können, so widerspricht dies nicht dem Grundsatz von Treu und Glauben.

e) Verarbeitung zu festgelegten Zwecken

Die Verarbeitung muss außerdem nach §47 Nr. 2 BDSG für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden.

Aus diesem Zweckbindungsgrundsatz resultiert, dass jegliche Datenverarbeitung nur dann erfolgen darf, wenn der Zweck zum Zeitpunkt der Datenerhebung bereits fixiert wurde.[177] Dies schließt eine Datenerhebung, bei denen die Zwecke erst zukünftig festgelegt werden, aus.[178] Gleichermaßen darf keine willkürliche Verarbeitung zu anderen Zwecken als für diejenigen, für welche die Datenerhebung stattfand, erfolgen.[179] Der Zweck selbst, der für die Datenerhebung festgelegt wird, muss neben dem Kriterium der Rechtmäßigkeit auch die Anforderung der Eindeutigkeit erfüllen. Hinsichtlich der Rechtmäßigkeit ist diese im behördlichen Kontext zu bejahen, wenn die mit dem Zweck verbundene Aufgabe in den Kompetenzbereich der Behörde fällt und diese – gesetzlich legitimiert – erforderlicherweise aufgrund eines öffentlichen Interesses oder im Rahmen strafprozessualer Maßnahmen ausgeführt wird.[180] Vorliegend wird die Einwilligung in eine strafprozessuale

[177] Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 12; Müller in Lisken/Denninger PolR-HdB, Kapitel G Rn. 600
[178] Braun in Gola/Heckmann, DS-GVO BDSG, §47 BDSG Rn. 13
[179] Frenzel in Paal/Pauly, DS-GVO BDSG, Art. 5 DSGVO Rn. 30
[180] Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 12

Maßnahme untersucht, welche folglich einem rechtmäßigen Zweck dienen.

Die Eindeutigkeit des Zweckes gilt als erfüllt, wenn der Zweck derart konkret formuliert ist,[181] so dass bei dessen Betrachtung vernünftigerweise keine Fehlinterpretationen entsteht oder Fehlschlüsse begünstigt werden, weil der Zweck eine hinreichende Spezifizierung erfahren hat.[182]

f) Verhältnismäßigkeit der Verarbeitung

Nach §47 Nr. 3 BDSG muss die Verarbeitung der personenbezogenen Daten einer Verhältnismäßigkeitsprüfung standhalten.

Dabei muss die vorzunehmende Verarbeitung auch dem festgelegten Verarbeitungszweck entsprechen, die Verarbeitung für das Erreichen des Verarbeitungszweckes erforderlich sein und gleichzeitig nicht außer Verhältnis zum Zweck stehen.[183]

Der legitime Zweck ergibt sich aus dem in §45 BDSG festgelegten Anwendungsbereich, die Verarbeitung zum Zwecke der Erfüllung von Aufgaben für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten. Umgekehrt bedeutet dies, dass wenn eine Polizeibehörde einem Betroffenen eine Maßnahme anbietet, die nicht zu Erfüllung einer der aufgeführten Aufgaben führt, jedenfalls kein legitimer Zweck nach Maßgabe des §47 Nr. 3 BDSG vorliegt.[184] Da vorliegend eine Einwilligung in eine strafprozessuale Maßnahme untersucht wird, gilt das Vorliegen eines legitimen Zweckes als vorausgesetzt.

Ferner muss der Zweck und die Verarbeitung auch im Weiteren dem Verhältnismäßigkeitsgrundsatz entsprechen, also auch erforderlich und angemessen sein.[185] Dies ist auch Konsequenz der grundsätzlichen

[181] Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 12
[182] Pötters in Gola/Heckmann, DS-GVO BDSG, Art. 5 DSGVO Rn. 15 Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 76
[183] Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 14
[184] vgl. ErwG 29 JI-RL; Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 15
[185] Braun in Gola/Heckmann, DS-GVO BDSG, §47 BDSG Rn. 16-19

Erfordernis der Rechtfertigung, welcher jeder vorzunehmende Grundrechtseingriff zu berücksichtigen hat.[186] Erforderlich ist die Maßnahme, wenn kein milderes, gleichwirksames Mittel vorliegt, was im Datenschutzkontext auch das Prinzip der Datenminimierung begründet.[187] Erforderlich ist also immer nur gerade die Datenmenge, die benötigt wird um den festgelegten Zweck zu erreichen. Außerdem muss sich die Datenmenge auf diejenigen Daten beschränken, welche dem Zweck überhaupt dienlich sind.[188] Im Umkehrschluss bedeutet dies, dass ein Datum nur verarbeitet werden darf, wenn ohne die Verarbeitung der Zweck nicht erfüllt werden kann.[189]

Die Prüfung der Angemessenheit schließlich wird das gewählte mildeste Mittel in unmittelbare objektive Relation zum zu erreichenden Zweck gesetzt.[190] In der Abwägung enthalten sein muss im Wesentlichen jeder Umstand, welcher im Kontext der Verarbeitung eine zu gewichtende Rolle spielt. Dazu zählt vor allem das Ausmaß der Verarbeitung hinsichtlich eines zu verhindernden Exzesses,[191] die Art der personenbezogenen Daten unter Berücksichtigung der Eingriffstiefe und vor allem die Folgen der Verarbeitung für die betroffene Person.[192] Insbesondere auch die Kombination mehrerer vorzunehmender Verarbeitungen, die jede für sich genommen einen Eingriff darstellt, muss im Kontext berücksichtigt werden.[193]

Wird einem angehaltenen Autofahrer etwa ein Test zur Messung des Atemalkohols angeboten, so ist die Datenerhebung auf den für die Zweckerreichung erforderlichen Maßnahmen zu reduzieren, insofern der Fahrer eingewilligt hat. Eine zusätzliche Befragung der Konsumhistorie des Fahrers steht möglicherweise noch in unmittelbarem Zusammenhang mit der Messung und dient aufgrund des Indizcharakters dem Zweckziel, der Sicherstellung der Fahrtauglichkeit des Fahrers. Eine separate

[186] Müller in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 601
[187] Braun in Gola/Heckmann, DS-GVO BDSG, §47 BDSG Rn. 17
[188] Reimer in Sydow/Marsch, DS-GVO | BDSG, Art. 5 DSGVO Rn. 33, 34
[189] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 121
[190] Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 19
[191] Schantz in BeckOK DatenschutzR, Art. 5 DSGVO Rn. 26
[192] Müller in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 602
[193] Braun in Gola/Heckmann, DS-GVO BDSG, §47 BDSG Rn. 20

Rechtsgrundlage ist aber notwendig, wenn darüber hinaus noch die Lautstärke des Fahrzeugs überprüft werden soll. Dies widerspricht nicht dem Vorliegen eines legitimen Zwecks, dieser müsste aber für sich neu begründet werden.[194] Fällt das Messergebnis in beiden Fällen so aus, dass die Fahrt bedenkenlos fortgesetzt werden kann, so verbietet es sich die resultierenden Messergebnisse in einer polizeilichen Datenbank in Verbindung mit der Identität der betroffenen Person oder Daten, welche Rückschlüsse auf die Identität zulassen, zu speichern, da diese nicht weiter benötigt werden.[195] Eine Verhältnismäßigkeitsprüfung ist bei jedweder Verarbeitung von personenbezogenen Daten durchzuführen,[196] auch wenn die Rechtsgrundlage die Einwilligung darstellen soll.[197]

g) Richtigkeit und Aktualität der Daten

Nach §47 Nr. 4 BDSG müssen die verarbeiteten personenbezogenen Daten auch einer sachlichen Richtigkeit unterliegen und außerdem im Falle eines vorliegenden Erfordernisses dem neusten Stand entsprechen. Dabei sind alle Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Sachliche Richtigkeit unter Beachtung von Art und Zweck der Verarbeitung erfährt ein Datum, wenn objektive Übereinstimmung mit den im Datum enthaltenen Informationen besteht. Eine rein behördliche Validierung der Daten ist für die Richtigkeit hingegen nicht ausreichend, insofern es sich nicht um Tatsachen, sondern um Werturteile handelt.[198] Aus §73 BDSG ergibt sich für die Polizeibehörde als verantwortliche Stelle die Maßgabe, wann immer möglich, zwischen Tatsachen und persönlichen Einschätzungen zu differenzieren und dies auch kenntlich zu machen. Auch bezieht sich die sachliche Richtigkeit bei getätigten Aussagen von Betroffenen gegenüber der Polizei auf die tatsächliche Vornahme der Aussage, nicht aber auf den Wahrheitsgehalt der

[194] Müller in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 600
[195] Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 130
[196] Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 17
[197] Schantz in BeckOK DatenschutzR, Art. 5 DSGVO Rn. 26
[198] Müller in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 494

Aussage.[199] Weiter ist von der Behörde eine Einkategorisierung der betroffenen Person nach §72 BDSG sachlich richtig vorzunehmen, insoweit die Möglichkeit dazu besteht. Soll eine betroffene Person im Rahmen der Ermittlungen als Zeuge befragt werden, so darf diese nicht ohne weiteres als Verdächtiger oder Straftäter kategorisiert werden.[200] Die Richtigkeit eines Datums ist bei der initialen Speicherung mit dem objektiv notwendigen Maß an Sorgfalt zu überprüfen, eine später festgestellte Richtigkeitsabweichung gleichermaßen der Korrektur zuzuführen.[201]

Bietet eine Polizeibehörde einer betroffenen Person eine Maßnahme an und willigt diese sein, so sind die Durchführungsresultate gewissenhaft zu dokumentieren. Ergeben sich im Nachhinein Anhaltspunkte oder Tatsachen dafür, dass ein solches Resultat möglicherweise nicht richtig ist oder nicht richtig aufgenommen wurde, so ist dies zu korrigieren oder dem Umstand jedenfalls nachzugehen und dies entsprechend zu vermerken.[202]

h) Erforderliche Speicherdauer der Daten

Nach §47 Nr. 5 BDSG dürfen[203] personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke für die sie erhoben wurden, erforderlich ist. Dies gilt, wenn für die Dauer der Speicherung eine Speicherform gewählt worden ist, welche die Identifizierung der betroffenen Personen auch ermöglicht.

Der Grundsatz der Speicherbegrenzung stellt somit die temporale Konkretisierung der festgestellten Grundsätze von Zweckbindung und Verhältnismäßigkeit dar[204] und begünstigt dadurch die Datensparsamkeit.[205] Die Behörde als Verantwortlicher hat demnach

[199] vgl. ErwG 30 JI-RL; Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 22
[200] Braun in Gola/Heckmann, DS-GVO BDSG, §47 BDSG Rn. 24
[201] Wolff in Schantz/Wolff, Das neue Datenschutzrecht Rn. 442
[202] Wolff in Schantz/Wolff, Das neue Datenschutzrecht Rn. 442
[203] Der Wortlaut spricht von „müssen“, s. auch Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 27
[204] Pötters in Gola/Heckmann, DS-GVO BDSG, Art. 5 DSGVO Rn. 26
[205] Albrecht in Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Teil 2: Grundsätze der DSGVO Rn. 6

bereits bei Datenerhebung eine definierte Frist zu berücksichtigen, nach welcher sie die gespeicherten Daten auf Notwendigkeit der Speicherfortbestehung prüft.[206] Ist im Zeitpunkt der Überprüfung eine Speicherung nicht mehr notwendig, so sind die betroffenen Daten der Löschung zuzuführen[207] oder jedenfalls durch Anonymisierung den Personenbezug zu eliminieren.[208] Vom Grundsatz der Speicherbegrenzung und der daraus resultierenden Löschpflicht ist grundsätzlich unabhängig der Rechtsgrundlage zu betrachten und umfasst damit auch die auf einer Einwilligung basierende Datenspeicherung, jedenfalls wenn keine Erforderlichkeit mehr besteht, das Datum weiter zu speichern. Wird also beispielsweise eine auf einer Einwilligung basierende Aussage im Rahmen polizeilicher Ermittlungen nach §483 S.1 StPO aufgenommen, im anschließenden Strafprozess aber nicht weiter berücksichtigt, so ist nach Abschluss des Verfahrens nach §489 Abs. 1 Nr. 1 StPO eine Löschung vorzunehmen, da der ursprüngliche Zweck der Datenverarbeitung weggefallen ist.[209]

i) Sicherheit der Verarbeitung

Nach §47 Nr. 6 BDSG muss die Verarbeitung der personenbezogenen Daten eine angemessene Sicherheit gewährleisten. Insbesondere sind hierfür geeignete technische und organisatorische Maßnahmen zu treffen, welche einen ausreichenden Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung bieten.

Eine Verarbeitung personenbezogener Daten darf also grundsätzlich nur erfolgen, wenn ein angemessenes Niveau an Sicherheit auch gegenüber dem Betroffenen gewährleistet werden kann. Fehlt es an einem solchen Niveau darf auch keine Einwilligung zur Datenverarbeitung eingeholt werden, bzw. darf die auf der Grundlage der Einwilligung beruhende Verarbeitung nicht durchgeführt werden. Der technische Aufbau dieses

[206] Braun in Gola/Heckmann, DSGVO BDSG, §47 BDSG Rn. 26
[207] Wolff in Schantz/Wolff, Das neue Datenschutzrecht Rn. 444
[208] Kramer in Paschke/Berlin/Meyer/Kröner, Hamburger Kommentar Gesamtes Medienrecht, 76. Abschnitt Rn. 45
[209] VGH Mannheim, Urteil v. 30.11.2016 – 1 S 472/16

Niveaus ist dabei nach §64 Abs. 1 BDSG am Stand der Technik zu bemessen, welcher seinerseits wiederum im Verhältnis seiner Implementierungskostens und der von der Verarbeitung ausgehenden Risiken für die Rechte und Freiheiten der betroffenen Personen zu betrachten ist.[210] Der Stand der Technik selbst ist nicht legal definiert, wird nach der Rechtsprechung aber zwischen den anerkannten Regeln der Technik und dem Stand von Wissenschaft und Technik eingeordnet.[211] Die aktuelle Bestimmung des Standes der Technik bemisst sich dabei etwa an den Vorgaben des Bundesministeriums für Sicherheit in der Informationstechnik (BSI)[212] oder den Empfehlungen des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT)[213]. Weiter führt §64 Abs. 2 BDSG an, dass Maßnahmen zur Pseudonymisierung und Verschlüsselung getroffen werden können, insofern eine Umsetzungsmöglichkeit besteht. Eine Pflicht zur Implementierung dieser Maßnahmen besteht dabei nach dem Wortlaut nicht, allerdings gilt es die Berücksichtigung der Implementierungsmöglichkeit beim Treffen der Maßnahmen grundsätzlich vorzunehmen.[214] Gleichzeitig gibt Abs. 2, Nr. 1 die durch Abs. 1 bezweckten Schutzziele vor: Verfügbarkeit (die Zugänglichkeit der Daten[215]), Vertraulichkeit (der ausschließlich befugte Zugriff auf die Daten[216]) und Integrität (die Gewährleistung der inhaltlichen Nichtveränderung der Daten[217]) der personenbezogenen Daten,[218] sowie im weiteren die Belastbarkeit der Systeme und Dienste, welche im Rahmen der Verarbeitung personenbezogener Daten herangezogen werden. Die Belastbarkeit von Systemen ist hierbei als Ausprägung der Resilienz zu verstehen, also der Erkennung und

[210] Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 30
[211] Piltz in Kipker/Reusch/Ritter, Recht der Informationssicherheit, Art. 32 DSGVO Rn. 15; BVerfG, Beschluss v. 08.08.1978 – 2 BvL 8/77
[212] bspw. die vom BSI herausgegebenen Technischen Richtlinien: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/technische-richtlinien_node.html; abgerufen am 03.08.2023; Braun in Gola/Heckmann, DSGVO BDSG, §47 BDSG Rn. 28
[213] s. hierzu https://www.teletrust.de/publikationen/broschueren/stand-der-technik/; abgerufen am 03.08.2023
[214] Bock in BeckOK DatenschutzR, §64 BDSG Rn. 40
[215] Sohr in Kipker, Cybersecurity, Kapitel 3 Rn. 10
[216] Cashor in Borges/Meents, Cloud Computing, §10 Datensicherheit Rn. 3
[217] Martini in Paal/Pauly, DS-GVO BDSG, Art. 32 DSGVO Rn. 36
[218] Bock in BeckOK DatenschutzR, §64 BDSG, Rn. 6ff

Reaktion auf Ausfälle oder Angriffe hinsichtlich Widerstandsfähigkeit und Wiederherstellbarkeit.[219] Zusätzlich wird in Abs. 3 ein Anforderungskatalog mit speziellen Zweckzielen festgelegt, welche nach Durchführung einer Risikoanalyse im Einzelfall zu erfüllen sind.[220] Insbesondere die Verschlüsselung wird in Abs. 3 S. 2 – trotz keiner ausdrücklichen Pflicht zur Vornahme dieser – nochmalig als valide Möglichkeit zur Entgegnung von Gefährdungen und Erfüllung der Anforderungen explizit benannt.

Der grundsätzliche Einsatz einer technisch-organisatorischen Maßnahme bestimmt sich somit regelmäßig individuell und risikobasiert.[221] Die Rechtsgrundlage, welche die Datenverarbeitung begründet, spielt jedoch hinsichtlich der zu treffenden Maßnahmen keine Rolle. Die Behörde muss also alle technisch wie organisatorischen Maßnahmen nach §64 BDSG heranziehen, welche nach der vorgenommenen Analyse der Verarbeitung zur Etablierung des Sicherheitsniveaus verhältnismäßig sind.

j) Zwischenergebnis

Die Grundsätze der Datenverarbeitung sind durch die verarbeitende Behörde in jedem Falle sicherzustellen. Dabei ist die Umsetzung bereits vor der schlussendlichen Verarbeitung zu bedenken. Für den zu betrachtenden Sachverhalt bedeutet dies, dass bevor für eine Verarbeitung eine Einwilligung angeboten werden kann, die Rahmenparameter bereits umfassend festgelegt sein müssen. Eine polizeiliche Maßnahme darf dabei nicht willkürlich erfolgen, sondern muss rechtmäßig sein und muss bei gleichzeitiger Verhältnismäßigkeit dabei festgelegten Zwecken entsprechen. Diese ist unter Berücksichtigung des Grundsatzes von Treu und Glauben dabei vor Verarbeitungsbeginn festzustellen. Weiter muss die Speicherdauer auf das erforderliche Maß beschränkt werden und die der Verarbeitung

[219] Mantz in Sydow/Marsch, DS-GVO | BDSG, Art. 32 DSGVO Rn. 17
[220] Schmieder in Forgó/Helfrich/Schneider, Betr. Datenschutz, Kapitel 2 Rn. 44
[221] Piltz in Kipker/Reusch/Ritter, Recht der Informationssicherheit, Art. 32 DSGVO Rn. 36

zugrundeliegenden personenbezogenen Daten durch technische und organisatorische Maßnahmen angemessen geschützt sein. Nur nach umfassender und nachweislicher Einhaltung der Grundsätze darf die Datenverarbeitung durch die Behörde vorgenommen werden.

F. Datenschutzrechtliche Einwilligung

Nach der Erläuterung der Datenschutzgrundsätze, die in jedem Fall durch die verantwortliche Behörde eingehalten und umgesetzt werden müssen, wenn eine Verarbeitung auf Grundlage der Einwilligung eines Betroffenen stattfinden soll, gilt es nun die einzelnen Bestandteile der Einwilligung und deren genaue Voraussetzungen detailliert zu beleuchten.

Die Voraussetzungen unter denen eine Einwilligung für die Verarbeitung personenbezogener Daten im festgestellten Anwendungsbereich bei einem Betroffenen eingeholt werden kann sind in §51 BDSG normiert. §51 BDSG bildet dabei allerdings keine eigenständige Rechtsgrundlage. Nach §51 Abs. 1 1. HS BDSG kann eine Einwilligung nur eingeholt werden, wenn dies aufgrund einer anderen Rechtsvorschrift normiert wurde. Wird demnach durch die Behörde von der Möglichkeit der Einwilligungseinholung eines Betroffenen Gebrauch gemacht, so ist die Umsetzung nur nach Maßgabe des §51 BDSG legitim.[222]

Zuvor wurde die Einwilligung selbst in §47 Nr. 17 BDSG bereits definiert. Demnach ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Diese Definition entspricht Art. 4 Nr. 11 DSGVO und folgt dem Gedanken des

[222] Schwichtenberg in Kühling/Buchner, DS-GVO BDSG, §51 BDSG Rn. 1

ErwG 35 JI-RL, welcher die zu behandelnde Einwilligung ebenfalls im Sinne der Datenschutzgrundverordnung betrachtet.[223]

Die Möglichkeit zur Anwendung der Einwilligung als datenschutzrechtliche Rechtfertigung basiert dabei nicht aus den in der JI-Richtlinie aufgeführten Umsetzungsvorschriften. Vielmehr wird die Option der Einholung der Einwilligung einer betroffenen Person lediglich durch deren Erwägungsgründe aufgebracht, wodurch eine grundsätzliche Vereinbarkeit der Vorschriftenkonstitution begründet wird.[224] Die nicht explizite Nennung der Einwilligung als mögliche Rechtsgrundlage in der JI-RL rührt wohl eher daher, dass es den umzusetzenden Mitgliedsstaaten selbst überlassen werden sollte, die Einwilligung in Rahmen der Strafverfolgung als begründende Verarbeitungsmöglichkeit zu konstituieren, insofern die weiteren Voraussetzungen der JI-RL eingehalten werden.[225]

Die JI-Richtlinie zählt in ErwG 35 - betont nur exemplarisch - die Zustimmung zu DNS-Tests oder zur Überwachung mittels elektronischer Fußfessel auf. Weiter spricht ErwG 37 JI-RL von der grundsätzlichen Möglichkeit auch eine Einwilligung für die Verarbeitung von personenbezogenen Daten, welche ihrem Wesen nach eine besondere Sensibilität hinsichtlich der Grundrechte und Grundfreiheiten Betroffener aufweist. Allerdings gibt der Erwägungsgrund gleichermaßen auf, dass auch hier eine nationale Rechtsvorschrift die Verarbeitung erlauben muss und nicht allein die Abgabe der Einwilligung durch den Betroffenen für die Verarbeitung legitimierend wirken soll.[226]

Im Folgenden werden nun die exakten datenschutzrechtlichen Anforderungen überprüft, die sich im speziellen aus den Vorschriften des BDSG, insbesondere aus §51 ableiten lassen. Diese werden im Kontext der in der StPO geregelten strafprozessualen Maßnahmen betrachtet und ob deren Vereinbarkeit untersucht.

[223] Schwichtenberg in Kühling/Buchner, DS-GVO BDSG, §51 BDSG Rn. 2
[224] Schwichtenberg in Kühling/Buchner, DS-GVO BDSG, §47 BDSG Rn. 7
[225] Schantz in Schantz/Wolff, Das neue Datenschutzrecht, Rn. 538
[226] Heckmann in Gola/Heckmann, DSGVO BDSG, §51 BDSG Rn. 10

I. Voraussetzungen der Einwilligung nach §51 BDSG

a) Vorliegen einer Rechtsvorschrift

Nach §51 Abs. 1 1. HS BDSG muss für die Einschlägigkeit der Vorschrift zunächst eine andere Rechtsvorschrift bestehen, welche die Einwilligung als mögliche Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten vorsieht. In Bezug auf die zu untersuchende Einwilligung in polizeiliche Ermittlungen straffprozessualer Natur kommt hier vorrangig die StPO als Legitimationsgrundlage in Betracht.

Unterliegt eine Einwilligungsvorschrift nicht den voraussetzenden Anforderungen des §45 BDSG, so kann auch §51 BDSG nicht angewendet werden.[227] Dies ist insbesondere der Fall, wenn die Behörde privatrechtlich handelt,[228] aber auch wenn ein Betroffener eine Anzeige bei einer Online-Wache abgibt. Diese löst zwar möglicherweise strafrechtliche Ermittlungen aus, im Zeitpunkt der Abgabe gelten aber die Voraussetzungen der DSGVO.[229]

Die StPO jedoch führt in ihren Vorschriften nur an wenigen Stellen eine explizit verankerte Rechtsgrundlage der Einwilligung in strafprozessuale Maßnahmen.[230] Es werden in erster Linie Voraussetzungen geschaffen, welche die Maßnahmendurchführung in erforderlichen Fällen normiert. §81a StPO etwa regelt die körperliche Untersuchung von Beschuldigten, welche nach Abs. 2 durch einen Richter oder bei Gefahr im Verzug von der Staatsanwaltschaft oder deren Ermittlungspersonen angeordnet werden kann. Die Voraussetzung der richterlichen Anordnung oder des begründeten Erfordernisses einer Gefahr im Verzug widerspricht nicht grundsätzlich dem Verständnis vom Beschuldigten eine Einwilligung einzuholen, um diesen körperlich zu durchsuchen.[231] Immerhin kann eine solche Untersuchung grundsätzlich auch einer möglichen Entlastung eines Beschuldigten dienen. Ordnet der Richter keine körperliche

[227] Stemmer in BeckOK DatenschutzR, §51 BDSG Rn. 1.
[228] etwa die Einholung der Einwilligung für die Zusendung von Infomaterialien
[229] Frenzel in Paal/Pauly, DS-GVO BDSG, §51 BDSG Rn. 3
[230] etwa §81h StPO (DNA-Reihenuntersuchung)
[231] Goers in BeckOK StPO, §81a StPO Rn. 16

Durchsuchung an, ist dies nicht gleichbedeutend damit, dass ein Beschuldigter seinen Beschuldigtenstatus verliert. Vielmehr können sich möglicherweise auch bereits auf andere eindeutige sachverhaltsdienliche Beweise gestützt werden,[232] so dass das Ergebnis einer zusätzlichen körperlichen Durchsuchung hinsichtlich eines Strafprozesses unerheblich bzw. aus ermittlungsrichterlicher Sicht nicht verhältnismäßig wäre und deshalb unzulässig erscheint.[233] Ablehnungsgründe können gleichermaßen auch weitere formelle Fehler bei der Antragstellung durch die Staatsanwaltschaft sein,[234] welche der Ermittlungsrichter nur in offenkundigen Fällen eigeninitiativ heilen kann.[235] Andersrum kann aber ein mögliches entlastendes Resultat bei der Anwendung einer solchen Maßnahme sehr wohl eine prozessuale Rolle spielen. Es erscheint daher nicht nachvollziehbar, warum einem Beschuldigten nur wegen des Fehlens einer expliziten normativen Einwilligungsmöglichkeit in eine Maßnahme die Möglichkeit genommen werden soll, sich durch polizeiliche Maßnahmen auch selbst zu entlasten. Freilich gilt auch bei einem Verweigern der Einwilligung und gleichzeitiger Nichtanordnung einer körperlichen Durchsuchung die sich aus dem Rechtsstaatsprinzip sich ergebende Unschuldsvermutung.[236] Der Betroffene kann jedoch entlastende Tatsachen vorbringen, um damit auch weitere ermittelnde Maßnahmen gegen ihn auszusetzen oder gegenstandlos zu machen und so möglicherweise auch weitere strafprozessuale Unannehmlichkeiten zu verhindern, da ein hinreichender Tatverdacht nicht mehr angenommen wird.[237] Dies gilt umso mehr, da eine strafrechtliche Beurteilung der Handlung des Betroffenen durch die Ermittlungsbehörden trotz der Unschuldsvermutung zulässig ist,[238] auch wenn diese nicht als Täter bezeichnet werden dürfen.[239]

[232] Frister in Lisken/Denninger, PolR-HdB, Kapitel F Rn. 118
[233] Weingarten in KK-StPO, §162 StPO Rn. 19
[234] Kölbel in MüKo-StPO, §162 StPO Rn. 19ff
[235] Weingarten in KK-StPO, §162 StPO Rn. 6
[236] Beukelmann, NJW-Spezial 2016, 696
[237] Jarass, GrCH, Art. 48 Rn. 19
[238] BVerfG, Beschluss v. 29.05.1990 – 2 BvR 254/88, 2 BvR 1343/88
[239] Frister in Lesken/Denninger, PolR-HdB, Kapitel F Rn. 119

§81b StPO regelt die Vornahme der erkennungsdienstlichen Behandlung bei Beschuldigten. In Abs. 1 der Vorschrift wird die Möglichkeit eingeräumt, vom Beschuldigten auch „gegen seinen Willen“ Lichtbilder anzufertigen und Fingerabdrücke abzunehmen. Aus dem nicht abschließend formuliert gestalteten Wortlaut und unter Hinzuziehung des §41 PolG (BW)[240] ergibt sich, dass vom Anwendungsbereich der Norm auch weitere Maßnahmen umfasst sind.[241] Dazu zählen etwa das Vermessen oder Ablichten einzelner Körperteile[242] oder Auffälligkeiten wie Tätowierungen,[243] nicht etwa aber die Entsperrung von Mobilgeräten mittels Fingerabdruck.[244] Bei Anwendung eines Umkehrschlusses kann folglich angenommen werden, dass es dann auch grundsätzlich möglich sein muss eine solche Vornahme „im Willen“, also mit Einwilligung des Beschuldigten zu tätigen.[245] Ähnlich verhält es sich auch mit weiteren Vorschriften, etwa §81c (Untersuchung anderer Personen) oder §81f (Verfahren bei der molekulargenetischen Untersuchung), bei denen die Verrichtung der Maßnahme dem Wortlaut nach auch „ohne Einwilligung der betroffenen Person“ vorgenommen werden darf. Auch hier kann der Annahme gefolgt werden, die Vorschrift dahingehend auszulegen, eine Maßnahme dann auch bei Vorliegen einer Einwilligung regelmäßig möglich sein muss.[246] Dogmatisch unerheblich ist dabei, ob eine Einwilligung überhaupt praxisrelevant wäre, da das grundsätzliche Vorliegen einer entsprechenden Einholungs- oder Abgabemöglichkeit der Einwilligung für die Beurteilung maßgeblich ist.

Fraglich ist also inwieweit die StPO die Möglichkeit der Einwilligung nach Maßgabe des §51 Abs. 1 BDSG nun tatsächlich explizit vorsehen muss oder ob der Rückschluss auch implizit dem Charakter der Norm entnommen werden kann. Der Wortlaut des §51 Abs. 1 BDSG spricht

[240] Polizeigesetz von Baden-Württemberg exemplarisch, Parallelvorschriften anderer Länder bspw. Art. 14 BayPAG (Bayern), §19 HSOG (Hessen), §15 NPOG (Niedersachsen), §14 PolG NRW (Nordrhein-Westfalen)
[241] Trück in MüKO-StPO, §81b StPO Rn. 16
[242] Vgl. §41 Abs. 2 Nr. 4 PolG; VG Cottbus, Beschluss v. 14.02.2018 – VG 3 L 95/18
[243] Vgl. §41 Abs. 2 Nr. 3 PolG; OVG Lüneburg, Beschluss v. 17.12.2004 – 11 ME 264/04
[244] Sieder/Brodowski in Hoeren/Sieber/Holznagel, MMR-HdB, Teil 19.3 Rn. 196
[245] VGH Mannheim, Urteil v. 07.03.2007 - 1 S 1170/05 bezogen auf §36 Abs. 1 Nr. 2 PolG a.F.
[246] Schieder, GSZ 2021, 16

ebenfalls nicht von einer expliziten Nennung der Einwilligungsmöglichkeit einer Rechtsvorschrift. Vielmehr muss die Berufung auf die Einwilligung nur nach der Vorschrift „erfolgen können“. Dies lässt den logischen Schluss zu, dass eine Einwilligung nach logischer Auslegung der Norm möglich ist, ohne dass diese in der Norm selbst ausdrücklich erwähnt wird.[247] Gründe hierfür können grundsätzlich, wie bereits erwähnt, eine durch den Betroffenen zu erreichende Entlastungswirkung sein oder auch die Verkürzung einer angesetzten strafprozessualen Maßnahme.

Auch der datenschutzrechtlich anerkannte Grundsatz des Verbots mit Erlaubnisvorbehalt widerspricht dem nicht. Da die Polizei als Ermittlungsperson der Staatsanwaltschaft grundsätzlich auch für die potenzielle Entlastung Beschuldigter zuständig ist, kann es mithin erforderlich sein dem Betroffenen eine Maßnahme anzubieten, insofern kein milderes Mittel mit gleichem Ergebnis zur Verfügung steht und die Maßnahme insgesamt verhältnismäßig erscheint.[248] Die für eine Datenverarbeitung durch die Behörde notwendige Erfüllung des Erforderlichkeitsgrundsatzes kann dahingehend ausgelegt werden, dass die Erforderlichkeit auch dann bestehen kann, wenn der Betroffene durch seine Einwilligung einen Umstand nachweisen will, welcher für diesen im strafprozessualen Rahmen günstig erscheint und die Maßnahme dazu auch geeignet ist.[249]

Weiter muss es einem Betroffenen auch grundsätzlich möglich sein über seine Grundrechte zu disponieren, etwa bei einer Einschränkung des Grundrechts auf Unverletzlichkeit der Wohnung gem. Art. 13 Abs. 1 GG.[250] Gleichermaßen soll er auch im Rahmen der Ausübung auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG entsprechend selbstbestimmt handeln können.[251] Bei Maßnahmen mit großer Eingriffsschwere muss aber eine eindeutige

[247] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 13
[248] Frister in Lisken/Denninger, PolR-HdB, Kapitel F. Rn. 118
[249] Hertfelder in BeckOK DatenschutzR, §47 BDSG Rn. 18f
[250] OLG Köln, Beschluss v. 26.01.2018 – 1 RVs 3/18
[251] Golla/Skobel, GSZ 2019, 140

Eingriffsgrundlage normiert sein, welche dann wiederrum eine Einwilligungsmöglichkeit auch indizieren kann.[252]

Zudem könnte selbst eine rein polizeiliche Vorladung eines Beschuldigten im Ermittlungsverfahren nach §163a StPO im Grunde die Einwilligung des Vorzuladenden erfordern, da eine Befolgung der Vorladung nicht zwingend ist.[253] Eine Rechtspflicht der Vorladung zu folgen, gilt nur im Falle einer staatsanwaltschaftlichen Vorladung gem. §163a Abs. 3 S.1 StPO, einer Vorladung eines Ermittlungsrichters nach §133 Abs. 1 StPO oder sich aus §399 Abs. 1 AO ergeben, wenn die Finanzbehörde im Ermittlungsverfahren selbst Verfahrensherrin ist und eine Vorladung anordnet.[254] Eine Aussagepflicht, die sich auf Angaben zur Sache bezieht, entsteht daraus allerdings nicht, da für den Beschuldigten insofern das Schweigerecht greift.[255]

Gehen durch eine polizeiliche Maßnahme belastende Beweise oder Indizien hervor, so kann der Beschuldigte die Maßnahme möglicherweise abkürzen in dem er sich bereit erklärt bei einer Maßnahme mitzuhelfen.[256] Bezogen auf die Datenverarbeitung ist allerdings davon auszugehen, dass diese durch die bloße Kooperation bedingt, nicht auf die Rechtsgrundlage der Einwilligung zu stützen ist, wenn die Maßnahme selbst ursprünglich im Rahmen der Amtsbefugnisse der Ermittlungsbehörden eingeleitet wurde.[257]

Maßnahmen, welche aus Vorschriften heraus erfolgen, welche weder eine explizite Einwilligungsmöglichkeit besitzen oder einen impliziten Einwilligungscharakter erkennen lassen, müssen allerdings differenziert betrachtet werden.[258] Zwar kann hier grundsätzlich in gleicher Weise argumentiert werden, dass einem Beschuldigten die Gelegenheit geboten

[252] Soiné, NStZ 2018, 497
[253] Kölbel in MüKO-StPO, §163 StPO Rn. 12
[254] Schlothauer in Müller/Schlothauer/Knauer, Münchner Anwaltshandbuch Strafverteidigung, §3 Ermittlungsverfahren, Rn. 9
[255] dazu ausführlich Huber, Grundwissen – Strafprozessrecht: Schweigerecht des Beschuldigten, JuS 2007, 711
[256] Schlothauer in Müller/Schlothauer/Knauer, MAH Strafverteidigung, Teil B §3 Ermittlungsverfahren, Rn. 24
[257] vgl. ErwG 35 JI-Richtlinie; Golla/Skobel, GSZ 2019, 140
[258] Singelnstein, NStZ 2020, 639

werden muss, auf seine Entlastung hinzuwirken, dieser kann jedoch auch noch im Nachhinein Stellung zur Sache nehmen oder Beweisanträge stellen.[259] Andererseits wirkt auch der Wortlaut von §51 Abs. 1 BDSG dadurch überdehnt. Liegen keine normativen Anhaltspunkte für die Einwilligungsmöglichkeit einer Maßnahme vor, so kann diese auch nicht „nach einer Rechtsvorschrift erfolgen".[260] Problematisch wäre wohl in diesem Zusammenhang besonders, wenn der Betroffene sich bei der Durchführung der Maßnahme nicht entlasten, sondern vielmehr belasten würde. Folglich wäre durch die Behörde eine Datenverarbeitung ohne Rechtsgrundlage erfolgt, was sich im späteren Strafprozess unter Umständen ungünstig auf den Strafprozess auswirken könnte, etwa aufgrund eines Beweisverwertungsverbotes.[261] Ferner würden hier wohl auch Ansprüche des Betroffenen gegenüber dem Staat entstehen, da durch die illegitime Datenverarbeitung dessen Grundrecht auf informationelle Selbstbestimmung verletzt wurde.[262] Auswirkungen hätte dies möglicherweise allerdings auch auf die zuvor argumentativ aufgeführte Einwilligung in eine Vernehmung. Da in §163a StPO die Einwilligung weder explizit noch implizit durch Umkehrschluss erkennbar aufzeigt, müsste auch hier der Maßstab neu bemessen werden.[263] Jedoch könnte hierauf wieder entgegnet werden, dass nach §163a Abs. 1 StPO der Beschuldigte vor Abschluss der Ermittlungen zu vernehmen ist, ihm je nach Schweregrad des Tatvorwurfs aber auch eine schriftliche Möglichkeit zur Stellungnahme geboten werden kann. Dies kann dahingehend ausgelegt werden, dass die Vernehmung auch grundsätzlich dazu dient dem Beschuldigten eine Möglichkeit zu bieten überhaupt zur Sache Angaben machen zu können, welche von den Ermittlungsbeamten für das weitere Verfahren zu den Akten gelegt werden.[264] Insofern besteht hier eine staatliche Pflicht vor der staatsanwaltschaftlichen Vermerkung des Ermittlungsabschlusses gem. §169a StPO, einem Beschuldigten ihm das Angebot zur Abgabe seiner

[259] Weingarten in KK-StPO, §163a StPO Rn. 8
[260] El-Ghazi, ZIS 2019, 110
[261] Hauschild in MüKo-StPO, §94 StPO Rn. 53
[262] Schantz in Schantz/Wolff, Kapitel F. Rn. 1255
[263] Singelnstein, NStZ 2020, 639
[264] Weingarten in KK-StPO, §163a StPO Rn. 3f

Sichtweise einzuräumen, gleich wohl dieser nicht verpflichtet ist dieses Angebot anzunehmen.[265] Durch das Angebot wird damit gleichermaßen auch der Anspruch auf rechtliches Gehör gewahrt.[266] Folglich kann zwar nicht durch Umkehrschluss, aber durch Auslegung nach Sinn und Zweck der Norm auch eine Einwilligungsmöglichkeit angenommen werden.[267]

Problematisch stellt sich die Sachlage aber bei anderen Vorschriften, etwa bei einer Durchsuchung nach Maßgabe der §102ff StPO dar. Hier wird eine Einwilligung weder explizit noch implizit in der Norm geführt, was zu einem Ausschluss der Erfüllungsmöglichkeit der geforderten Regelung in einer Rechtsnorm führt.[268] Dies betrifft auch die in der Einleitung erwähnte Atemalkoholkontrolle.[269] Jene wird ihrerseits aus §36 Abs. 5 StVO zur Bestimmung des Alkoholgehalts nach §24a Abs. 1 StVG abgeleitet[270] und ist nicht gesondert normiert, was der Einwilligung in eine Datenverarbeitung auf Grund einer Rechtsnorm entgegensteht.[271] Bei polizeibehördlichen Ermittlungen kann §36 Abs. 5 StVO allerdings nur zur Anwendung kommen, wenn neben der Ermittlung auch die Durchführung einer Verkehrskontrolle gewollt ist.[272]

Eine Einwilligungsmöglichkeit in verbotene Vernehmungsmethoden nach §136a StPO kann schon aufgrund des Verbotscharakters der Norm nicht angenommen werden.[273]

Durch die Anerkennung der Einwilligung als mögliche zur Datenverarbeitung legitimierende Rechtsgrundlage und der Festlegung von Erfüllungsmerkmalen in §51 BDSG durch den deutschen Gesetzgeber entfällt auch die Notwendigkeit einer Auslegungsbedürftigkeit des Art. 8 JI-RL. Dort wird von Teilen der

[265] Kölbel in MüKo-StPO, §163a StPO Rn. 14
[266] Weingarten in KK-StPO, §163a StPO Rn. 1
[267] Gusy, NVwZ 1991, 614
[268] Singelnstein, NStZ 2020, 639
[269] El-Ghazi, ZIS 2019, 110
[270] BT-Dr 13/1439, S.4; https://dserver.bundestag.de/btd/13/014/1301439.pdf; abgerufen am 17.09.2023; Euler in BeckOK OWiG, StVG §24a Rn. 6
[271] El-Ghazi, ZIS 2019, 110
[272] Hühnermann in Burmann/Heß/Hühnermann/Jahnke, Straßenverkehrsrecht, §36 StVO Rn. 12
[273] Schieder, GSZ 2021, 16

Literatur bisweilen ein strenger Vorbehalt des Gesetzes hineingelesen, welche ausschließlich eine explizite Einwilligungsmöglichkeit in einer Vorschrift als Legitimation für eine Datenverarbeitung ansieht.[274] §51 BDSG ist wie festgestellt keine eigene Rechtsgrundlage und somit auch keine generalisierende Erlaubnisnorm. Die Schaffung einer solchen Generalklausel könnte zwar die Problematik der Einwilligungsbefugnis des §51 BDSG klären,[275] im Sinne der JI-Richtlinie wäre eine solche Vorschrift allerdings auch nicht, da insbesondere der ErwG 35 nur eine Einwilligung in hinreichend bestimmte Datenverarbeitungen vorsieht.[276]

Eine Rechtsvorschrift i.S.d. §51 Abs. 1 1. HS BDSG kann also unter den aufgeführten Voraussetzungen grundsätzlich vorgefunden werden. Ist jedoch keine explizite Einwilligungsmöglichkeit vorgesehen und kann nicht etwa durch einen Umkehrschluss eine implizite Möglichkeit gelesen werden, so ist die Einwilligung in eine strafprozessuale Maßnahme nicht möglich.

b) Nachweispflicht der Einwilligung

Der Verantwortliche muss die Einwilligung der betroffenen Person, welche dieser aufgrund einer Rechtsnorm i.S.v. §51 Abs. 1 1. HS BDSG erteilt hat, nachweisen können.

Aus der Vorschrift des §51 Abs. 1 2. HS BDSG ergibt sich somit eine den Verantwortlichen treffende Beweislast hinsichtlich der erbrachten Einwilligung eines Betroffenen.[277] Etwaige Zweifel hinsichtlich der Abgabe der Einwilligung, die sich etwa in einem anschließenden Verfahren ergeben, muss der Verantwortliche mit der Nachweiserbringung der tatsächlichen Einwilligungsabgabe begegnen.[278] Demnach ist der Nachweis nicht nur gegenüber der betroffenen Person, sondern auch gegenüber dem Gericht zu erbringen.[279] Gleichermaßen entfaltet der Nachweis über die Einwilligung auch eine Schutzwirkung

[274] Stief, StV 2017, 470; Schwichtenberg, DuD 2016, 605
[275] Schieder, GSZ 2021, 16
[276] Golla/Skobel, GSZ 2019, 140
[277] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 14
[278] Heckmann/Paschke in Gola/Heckmann, DSGVO BDSG, §51 BDSG Rn. 34
[279] Frenzel in Paal/Pauly, DS-GVO BDSG, §51 BDSG Rn. 4

auf die verantwortliche Behörde, da die Abgabe der Einwilligung durch die betroffene Person so im weiteren Verlauf nicht angezweifelt werden kann.[280]

Eine konkrete Form des Nachweises ist hingegen nicht normativ vorgegeben und kann dadurch grundsätzlich dem Verantwortlichen obliegen.[281] Die Nachweisführung muss aber auch unter dem Grundsatz der Datensparsamkeit erfolgen, darf also nicht zu einer nicht Erhöhung der gespeicherten Datenmenge führen.[282] Insoweit dürfen für die Nachweiserbringung auch nur jene Daten gespeichert werden, welche erforderlich sind, um der Nachweispflicht zu genügen.[283] Die Erforderlichkeit der Erbringung des Nachweises in Schriftform ist durch den sich nicht konkretisierenden Wortlaut der Norm also gerade nicht gegeben. Es kann hierfür jede denkbare elektronische oder physische Dokumentationsmöglichkeit genutzt werden.[284] In Betracht kommende Nachweisformen, sind etwa die audio- oder audiovisuelle Aufnahme der Einwilligungserbringung auf einem elektronischen Datenträger.[285] Insbesondere in Deutschland ist aber auch eine Beweiserbringung durch Zeugen nach §245 Abs. 1 StPO grundsätzlich zulässig. Denkbar wäre also auch eine Bestätigung der abgegebenen Einwilligung durch einen oder mehrere Polizeibeamte, welche bei der Abgabe der betroffenen Person zugegen waren.[286] Eine jederzeitige unmittelbare Abrufbarkeit des Nachweises, bzw. dessen Inhalts, wie etwa noch in §28 Abs. 3a BDSG a.F. vorgesehen, ist hingegen nicht von der Nachweispflicht umfasst.[287]

Die Aufbewahrungsdauer des Nachweises ist unmittelbar an die dazugehörige Verarbeitung geknüpft. Ist der Verarbeitungszweck

[280] Frenzel in Paal/Pauly, DS-GVO BDSG, Art. 7 DSGVO Rn. 6
[281] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 14
[282] Heckmann/Paschke in Gola/Heckmann, DSGVO BDSG, §51 BDSG Rn. 35
[283] Artikel-29-Datenschutzgruppe, 17/DE WP 259 rev.01, S.24, https://www.datenschutzstelle.li/application/files/3615/3674/7263/wp259rev01_de.pdf; abgerufen am 17.09.2023
[284] Steinrötter in BeckOK IT-Recht, Art. 7 DSGVO Rn. 20
[285] Klement in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 7 DSGVO Rn. 44
[286] Heckmann/Paschke in Ehmann/Selmayr, DSGVO, Art. 7 DSGVO Rn. 74
[287] Schulz in Gola/Heckmann, DS-GVO BDSG, Art. 7 DSGVO Rn. 66

hinfällig, insbesondere im Hinblick auf abgeschlossene Ermittlungs- bzw. Strafverfahren und keine weiteren Rechtsansprüche erkennbar, so darf auch der tatsächliche Nachweis der Einwilligung nicht länger gespeichert werden.[288] Die Führung des Nachweises stellt insofern eine separate Verarbeitung dar, welche aufgrund der gesetzlichen Anforderung zur Nachweispflicht dadurch aber erforderlich wird und folglich ihre Rechtsgrundlage in §45 BDSG zur Erfüllung der polizeilichen Aufgaben im Rahmen der strafprozessualen Ermittlungen findet.[289]

Die verantwortliche Polizeibehörde ist folglich dazu verpflichtet, einen Nachweis gleich welcher Form darüber zu führen, mit welchem sie belegen kann, dass die betroffene Person ihre Einwilligung abgegeben hat. Kann eine Behörde einen solchen Nachweis nicht erbringen, kann somit eine rechtmäßige Datenverarbeitung nicht angenommen werden.[290]

c) Form der Einwilligung

Fraglich ist in welcher Form die verantwortliche Polizeibehörde die Einwilligung einzuholen hat.

Wie bereits für den Nachweis der Einwilligung festgestellt, so gilt auch für die Abgabe der Einwilligung selbst zunächst keinerlei Formerfordernis.[291] Ein Betroffener kann damit frei wählen, ob dieser mündlich in eine angebotene Maßnahme einwilligt oder etwa eine von der Polizei vorbereitete Einwilligungserklärung unterschreibt.[292] Auch die eigene schriftliche Verfassung einer Einwilligung durch den Betroffenen selbst ist denkbar, genau wie die elektronische Abgabe per E-Mail[293] oder durch Ankreuzen einer Checkbox auf einer Website.[294] Bei Einholung der Einwilligung auf elektronischem Wege, insbesondere

[288] Artikel-29-Datenschutzgruppe, 17/DE WP 259 rev.01, S.24, https://www.datenschutzstelle.li/application/files/3615/3674/7263/wp259rev01_de.pdf; abgerufen am 17.09.2023
[289] vgl. analog zur DSGVO: Steinrötter in BeckOK IT-Recht, Art. 7 DSGVO Rn. 21
[290] OVG Saarlouis, Beschluss v. 16.02.2021 – 2 A 355/19
[291] Johannes/Weihnhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 27
[292] Stemmer in BeckOK DatenschutzR, Art. 7 DSGVO Rn. 83
[293] Johannes/Weihnhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 30
[294] Schulz in Gola/Heckmann, DS-GVO BDSG, Art. 7 DSGVO Rn. 43

über eine Website ist auf die Barrierefreiheit[295] zu achten und eine Vorlesbarkeit durch entsprechende Applikationen zu begünstigen.[296]

Selbst eine konkludent abgegebene Einwilligung ist prinzipiell vorstellbar, insofern diese an ein offensichtliches Verhalten des Betroffenen geknüpft ist, aus welchem das Einverständnis zur Datenverarbeitung durch die Maßnahme hervor geht.[297] Ein Stillschweigen oder bloßes Dulden einer Maßnahme stellt hierbei allerdings eine unzulässige mutmaßliche Einwilligung und somit gerade keine konkludente Einwilligung dar.[298] Schreibt eine strafprozessuale Vorschrift allerdings eine ausdrückliche Einwilligung vor, so besteht hierbei keine Möglichkeit die Verarbeitung basierend auf einer konkludenten Einwilligung vorzunehmen.[299]

§51 Abs. 2 BDSG stellt allerdings spezifische Voraussetzungen für den Fall auf, dass eine Einwilligung schriftlich abgegeben wird. Nach deutschem Verständnis entspricht die Schriftform nach §126 BGB einer handschriftlichen Abgabe zumindest der Unterschrift des Betroffenen unter die zu erteilende Einwilligung in Papierform.[300] Der Umstand, dass §51 BDSG allerdings auf der JI-Richtlinie basiert, welche wiederum ihrerseits an die DSGVO angelehnt ist, macht eine weite Auslegung der Schriftform erforderlich.[301] ErwG 32 DSGVO erweitert dem Wortlaut nach das Schriftformverständnis auch auf die elektronische Einwilligungsabgabe und grenzt zunächst nur zur mündlichen Abgabe ab. Die elektronische Abgabe einer Einwilligung deckt sich jedoch nicht mit dem deutschen Verständnis der Schriftform und findet sich in §126b BGB als „Textform“ gesondert normiert wieder. Die „elektronische Form“ gem. §126a BGB wird dadurch gekennzeichnet, dass sie durch die Verwendung einer qualifizierten elektronischen Signatur erzeugt wird. Die elektronische Form nach Maßgabe der DSGVO und folglich auch

[295] i.S.d. Richtlinie (EU) 2016/2102, in Deutschland umgesetzt z.B. durch §12a BGG
[296] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, §51 BDSG Rn. 23
[297] Schulz in Gola/Heckmann, DS-GVO BDSG, Art. 7 DSGVO Rn. 42
[298] Johannes/Weihnhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 28
[299] Stemmer in BeckOK DatenschutzR, Art. 7 DSGVO Rn. 85
[300] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 15
[301] Johannes/Weihnhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 30

des BDSG umschließt sowohl die deutsche Textform als auch die deutsche elektronische Form.[302] Da sich die Schriftform nach unionsrechtlichem Verständnis wie festgestellt auf die elektronische Form erstreckt, sind also auch Einwilligungen mittels qualifizierter elektronischer Signatur vom Regelungsgehalt der Norm erfasst.[303]

§51 Abs. 2 BDSG regelt aber auch den Fall, dass sich eine erteilte Einwilligung auf mehr als einen zugrundeliegenden Sachverhalt beziehen soll. In einem solchen Fall muss das Ersuchen um die Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren Sprache erfolgen, was gleichzeitig eine Abgrenzung der Sachverhalte, die einer Einwilligung zugrunde liegen, bedingt.

Der Betroffene hat demgemäß eine generelle Möglichkeit die Einwilligungsabgabe in Schriftform vorzunehmen, ohne dass dies einer weiteren Begründung bedarf.[304]

Die Abgrenzung eines Sachverhaltes bemisst sich hierbei auf eine Verarbeitung, welche nicht Gegenstand einer Maßnahme ist.[305] Eine Einwilligung eines Betroffenen in eine körperliche Untersuchung nach §81a StPO kann sich also nicht auf die Entnahme einer DNS-Probe i.S.v. §81h StPO erstrecken. Gleichwohl kann ein anderer Sachverhalt aber auch einen Teil einer Maßnahme darstellen, welcher auf einer anderen Rechtsgrundlage als die der Einwilligung, beruht.[306] Beispielsweise kann die Entnahme einer Blutprobe oder einer anderen Körpersubstanz nach §81a StPO im Rahmen polizeilicher Ermittlungen erforderlich sein, weswegen sich die Rechtsgrundlage für die Datenverarbeitung bereits aus §45 BDSG ergibt. Im gleichen Zuge kann aber der Betroffene etwa einwilligen, dass der Arzt hierfür eine neuartige Untersuchungsmethode anwendet, insofern gewährleistet ist, dass diese die Regeln der ärztlichen Kunst befolgt und es zu keinen Nachteilen für die Gesundheit des

[302] Spindler/Dalby in Spindler/Schuster, Recht der elektronischen Medien, Art. 7 DSGVO Rn. 8
[303] Steinrötter in BeckOK IT-Recht, Art. 7 DSGVO Rn. 26
[304] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 15
[305] Frenzel in Paal/Pauly, DS-GVO BDSG, Art. 7 DSGVO Rn. 11
[306] Frenzel in Paal/Pauly, DS-GVO BDSG, Art. 7 DSGVO Rn. 11

Betroffenen kommt.[307] Somit müsste sich durch das aufgeworfene Trennungsgebot die Einwilligung auf die Untersuchungsmethode klar abgrenzbar darstellen von der grundsätzlichen Durchführung der polizeilichen Maßnahme aufgrund strafprozessualer Erfordernisse.[308]

Wird einem Beschuldigten seitens der Behörden eine einwilligungsfähige Maßnahme angeboten und damit einhergehend die Abgabe der Einwilligung ersucht, so muss sich die Behörde dabei einer verständlichen und leichten Form, sowie einer klaren Sprache bedienen.

Wird die Abgabe der Einwilligung etwa schriftlich ersucht, so muss die Behörde für eine optische Unterscheidung des Ersuchens vom Begleittext sorgen.[309] Eine solche Unterscheidung kann etwa durch eine andersartige Formatierung, die Wahl einer anderen Schriftgröße oder -art, einer farblichen Markierung oder einer Umrandung hergestellt werden.[310] Das behördliche Ersuchen muss für den Betroffenen also auch derart verständlich sein, dass ihm die an die Einwilligungsabgabe geknüpfte Datenverarbeitung bewusst ist.[311] Dies bedingt eine hinreichend bestimmte Formulierung seitens der Polizeibehörde, welche außerdem nicht verklausuliert sein darf und weiter auch keinen Spielraum für Interpretationen aufwerfen darf.[312] Die Sprache, die hierfür von der Behörde gewählt wird muss auch für Betroffene verständlich sein, die keine ausgeprägten Sprachkenntnisse haben, etwa weil diese die deutsche Sprache als Fremdsprache führen.[313] Zugrundeliegende Sätze sollen demnach nur eine geringe Komplexität aufweisen, während das verwendete Vokabular sich nicht unnötigerweise an Fremdwörtern oder der Fach- und Bildungssprache bedienen soll.[314] Dabei ist aber eine Verbalisierung des Ersuchens zwingend notwendig, da bei rein

[307] Hadamitzky in KK-StPO, §81a StPO Rn. 6
[308] Spindler/Dalby in Spindler/Schuster, Recht der elektronischen Medien, Art. 7 DSGVO Rn. 9
[309] Johannes/Weihnhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 31
[310] Taeger in Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 7 DSGVO Rn. 72
[311] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 17
[312] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 18
[313] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 18
[314] BVerwG, Beschluss v. 14.08.1974 – I B 3.74; Taeger in Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 7 DSGVO Rn. 68

bildlichem oder piktografisch erläuterndem Ersuchen keine Sprache im Sinne der Vorschrift vorliegt.[315] Die Formulierung des Einwilligungsersuchens in der möglichen abweichenden Muttersprache des Betroffenen ist allerdings nicht erforderlich, da in Deutschland nach §23 Abs. 1 VwVfG insoweit nur die deutsche Sprache als Amtssprache vorgesehen ist.[316] Eine Gleichsetzung mit der von §11 BGG geforderten „leichten" Sprache ist indes aber unzutreffend, da diese sich ausschließlich an Menschen mit geistigen und seelischen Behinderungen richtet,[317] wenngleich die einfache Sprache keinem Kriterium der Sprachschönheit unterliegt.[318] Im Einzelfall können einfache und leichte Sprache jedoch übereinstimmend sein, da davon auszugehen ist, dass sich die einfache Sprache auch nach dem vorgesehenen Empfängerkreis bemessen lässt und ihrerseits Ausprägung des Transparenzgrundsatzes ist.[319] Eine Eingrenzung des Empfängerkreises von behördlichen Einwilligungsersuchen ist jedoch fernliegend, da insbesondere Maßnahmen der Polizeibehörde grundsätzlich sämtliche Personen innerhalb des Zuständigkeitsbereiches adressieren können, was konsequenterweise eine generelle einfache und verständliche Sprache erforderlich macht.[320]

Gibt ein Betroffener dementsprechend eine schriftliche Einwilligung ab, welche sich auf mehr als einen Sachverhalt bezieht, so hat die Behörde beim vorhergehenden Ersuchen, dieses derart in deutscher Sprache zu formulieren, dass der Betroffene sich einer verständlichen Sprache ausgesetzt sieht und dies durch eine gestalterisch auffällige Abgrenzung zu anderen Sachverhalten flankiert wird.[321]

[315] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, Art. 7 DSGVO Rn. 80
[316] Taeger in Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 7 DSGVO Rn. 70
[317] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, Art. 7 DSGVO Rn. 80
[318] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 19
[319] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, Art. 7 DSGVO Rn. 81
[320] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, Art. 7 DSGVO Rn. 81
[321] Johannes/Weihnhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 29, 31

d) Widerruf der Einwilligung

Die betroffene Person hat gem. §51 Abs. 3 S.1 BDSG jederzeit das Recht ihre Einwilligung zu widerrufen. Gleichermaßen ist die betroffene Person aber vor Abgabe der Einwilligung zu unterrichten, dass ein Widerruf die Rechtmäßigkeit der aufgrund der Einwilligung erfolgten Datenverarbeitung nicht berührt wird.

Um das Grundrecht der informationellen Selbstbestimmung aus Art. 8 Abs. 1 EMRK, bzw. Art. 2 Abs. 1 GG i.V.m. Art.1 Abs. 1 GG zu wahren, kann ein Betroffener seine Einwilligung nach der Abgabe widerrufen.[322] Dies kann unabhängig der zugrundeliegenden Motivation des Betroffenen ohne eine weitere Angabe von Gründen erfolgen.[323] Auch der Zeitpunkt des Widerrufes ist vom Betroffenen frei wählbar und lässt keinerlei Verzögerungsfrist hinsichtlich des Wirksamwerdens zu.[324] Es ist dabei auch unerheblich ob die Einwilligung vom Betroffenen von Vorneherein nur für einen bestimmten Zeitraum vorgesehen war und er dies bei Abgabe der Einwilligung offenbarte[325] oder diese zunächst auf unbestimmte Zeit gelten sollte.[326] Der Einwilligungswiderruf kann auch schon unmittelbar nach Beendigung der Abgabe der Einwilligung erfolgen.[327] Dabei kann der Widerruf aus einer Erklärung des Betroffenen hervorgehen und muss nicht gesondert als solcher explizit gekennzeichnet sein.[328] Weiter ist nicht zwangsläufig die gleiche Form zur Ausübung des Widerrufs zu wählen, welche zuvor Übermittlungskanal für die Einwilligung war. Insofern gilt auch beim Widerruf die Formfreiheit, vorbehaltlich möglicher einschränkender Vorschriften, welche normenspezifisch getroffen werden können.[329] Gibt ein Betroffener gegenüber der Behörde zunächst etwa die Einwilligung zur Entnahme einer DNS-Probe, so kann dieser sowohl vor als auch nach

[322] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, §51 BDSG Rn. 33
[323] Steinrötter in BeckOK DatenschutzR, Art. 7 DSGVO Rn. 28
[324] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 20
[325] Tinnefeld/Conrad, ZD 2018, 391
[326] Taeger in Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 7 DSGVO Rn. 76
[327] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 21
[328] Johannes/Weihnhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 34
[329] Johannes/Weihnhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 34

der stattfindenden Entnahme auch durch Verwendung einfacher Sprache gegenüber den Polizeibeamten erklären, dass er die Verarbeitung seiner personenbezogenen Daten nicht länger wünscht.[330] Wichtig ist hierbei nur, dass der Widerruf für die Behörde auch erkennbar ist[331] und die Abgabe des Widerrufs nicht mit höheren Anstrengungen verbunden ist, als es die Abgabe der Erklärung war.[332] Beispielsweise darf die Polizeibehörde den Widerruf nicht an spezielle Arbeitszeiten knüpfen, insofern für die Erteilung der Einwilligung eine jederzeitige Abgabe möglich war.[333] Im Anschluss hat die Behörde die Datenverarbeitung unmittelbar einzustellen oder erst gar nicht einzuleiten. Ist die Datenverarbeitung durch die Behörden bereits begonnen worden, so wirkt der Widerruf ex nunc, also ab Eingang bei der Behörde und entzieht dieser damit die Rechtsgrundlage für eine weitere einwilligungsbasierte Verarbeitung.[334] Die zuvor durchgeführte Datenverarbeitung, welche auf der Einwilligung basierte, bleibt mithin rechtmäßig.[335] Dies gilt jedoch nicht für den Fortbestand der Daten im System der Behörde, welche nach Zugang des Widerrufes der Löschung bzw. Vernichtung zuzuführen.[336] Erfolgte durch die Behörde auch eine Weitergabe der Daten an eine weitere Behörde oder andere Dritte, so sind auch diese über die Pflicht zur sofortigen Beendigung der Verarbeitung und anschließenden Löschung der Daten hinzuweisen.[337]

Hierbei ist jedoch zu bedenken, dass infolge der Verarbeitung aufgrund einer erteilten Einwilligung grundsätzlich auch andere Rechtsgrundlagen für eine nachgelagerte Verarbeitung in Betracht kommen können.[338] Dies ist etwa der Fall, wenn der im Ermittlungsverfahren aufgebaute Datenbestand zur Gewinnung von Beweismaterial im Kontext des

[330] Klement in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 7 DSGVO Rn. 85
[331] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 21
[332] Steinrötter in BeckOK DatenschutzR, Art. 7 DSGVO Rn. 30
[333] vgl. EDPB, Leitlinie 05/2020 zur Einwilligung gem. Verordnung 2016/679 V. 1.1, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf; abgerufen am 21.09.2023
[334] Johannes/Weinhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 36
[335] Frenzel in Paal/Pauly, DS-GVO BDSG, §51 BDSG Rn. 6
[336] Ingold in Sydow/Marsch, DS-GVO | BDSG, Art. 7 DSGVO Rn. 48
[337] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 24
[338] Frenzel in Paal/Pauly, DS-GVO BDSG, §51 BDSG Rn. 6

Strafprozesses geführt hat. Widerruft ein Betroffener nun seine Einwilligung, so muss die Behörde die Daten nicht löschen oder vernichten, wenn die Verarbeitung dieser im Rahmen weiterer strafprozessualer Maßnahmen erforderlich scheint.[339]

Der Betroffene ist in jedem Fall im Vorfeld der Abgabe der Einwilligung über die Umstände aufzuklären, dass dieser ein jederzeitiges Widerrufsrecht hat und dass die Datenverarbeitung in Folge eines Widerrufs beendet wird.[340] In dieser Belehrung ist aber auch insbesondere auf die rechtlichen Auswirkungen der Einwilligungsabgabe einzugehen, um den Betroffenen in jedem Fall darüber aufzuklären, dass eine vorgenommene Datenverarbeitung bis zu seinem Widerruf gesetzlich legitimiert bleibt.[341] Die Überbringung der Informationen hinsichtlich des Widerrufes zum Betroffenen unterliegt wie die gesamte Einwilligung dabei auch keinen grundsätzlichen Formerfordernissen.[342] Es ist somit denkbar, dass ein Betroffener gegenüber der Polizei eine mündliche Einwilligung erteilt, nachdem dieser zuvor schriftlich über das Widerrufsrecht informiert worden ist. Die Belehrungspflicht des Betroffenen ergibt sich dabei nicht aus den allgemeinen Informationen zur Datenverarbeitung nach §55 BDSG, welche die verantwortliche Stelle gegenüber dem Betroffenen zu erbringen hat. Vielmehr stellt §51 Abs. 3 BDSG eine zusätzliche Gebotsnorm dar, die im speziellen Fall der Einwilligung ihre Anwendung findet.[343] Unterlässt die Behörde die Erbringung der Widerrufsinformationen vor Abgabe der Einwilligung des Betroffenen, so kann durch diesen keine wirksame Einwilligung erteilt und keine rechtmäßige Datenverarbeitung begründet werden.[344]

e) Freiwilligkeit der Einwilligung

Nach §51 Abs. 4 S. 1 BDSG kann die erteilte Einwilligung nur wirksam sein, wenn die Abgabe dieser auf der freien Entscheidung der betroffenen

[339] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 23
[340] Johannes/Weinhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 39
[341] Stemmer/Wolf in BeckOK DatenschutzrR, §51 BDSG Rn. 25
[342] Johannes/Weinhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 37
[343] Johannes/Weinhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 41
[344] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 25

Person beruht. Weiter gibt die Norm mit S. 2 noch eine Anweisung hinsichtlich der potenziellen Bestimmbarkeit der Freiwilligkeit: die Berücksichtigung der Umstände, unter denen die Einwilligung erteilt wurde.

(1) Grundsätze der Freiwilligkeit

ErwG 35 der JI-RL gibt dabei einen erste Interpretationshilfe. Ist eine betroffene Person aufgefordert, durch aktive Mitwirkung oder bloßes Erdulden einer polizeilichen Maßnahme, einer Rechtspflicht nachzukommen, so kann in dieser Konstellation keine Wahlfreiheit angenommen werden. Wird etwa nach §81a StPO die Entnahme einer Blutprobe angeordnet, so kann es aus datenschutzrechtlicher Perspektive dahinstehen, ob der Betroffene hierzu seine Einwilligung erteilt. Durch die vorliegende Anordnung besteht bereits eine Rechtsgrundlage zur Durchführung der Maßnahme, nach welcher der Betroffene diese zu dulden hat. Insofern kann konsequenterweise auch keine freie Entscheidung des Betroffenen angenommen werden, sollte eine Einwilligung seitens der Behörden angefragt oder seitens des Betroffenen abgegeben worden sein, während die Maßnahme bereits angeordnet wurde.[345]

Gleiches gilt auch wenn durch Verwehrung der Einwilligung eines Betroffenen für diesen eine nachteilige Konsequenzfolge ausgelöst würde.[346] Dies könnte etwa der Fall sein, wenn einem Betroffenen etwa nach §68b Abs. 1 Nr. 12 i.V.m. §463a Abs. 4 StPO angeboten wird zur Bestimmung seines ständigen Aufenthaltsortes eine elektronische Fußfessel zu tragen, bei gleichzeitiger Kundgabe, dass ohne Akzeptanz der Fußfessel die Einweisung in eine Haftanstalt zwingend folgend würde.[347] Dies ist schon allein deswegen anzunehmen, weil das Freiheitsrecht des Betroffenen im Fall der Einwilligung eine wesentlich geringere Eingriffsintensität erleiden würde,[348] während der

[345] Singelnstein, NStZ 2020, 639
[346] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, §51 BDSG Rn. 28
[347] Frenzel in Paal/Pauly, DS-GVO BDSG, §51 BDSG Rn. 2
[348] Hochmayr, NStZ 2013, 13

Aufenthaltsort sowohl mit Fußfessel, als auch in der Haftanstalt jederzeit gegenüber den Behörden transparent wäre, gleichwohl bei Letzterem wesentlich weniger Datenbestand erzeugt wird. Dem gegenüber steht zwar die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung, welches von einem Betroffenen aber regelmäßig als geringwertiger betrachtet werden dürfte, wenn dessen Alternative Freiheitsentzug durch Straf- oder Untersuchungshaft ist.[349] Dies auch insofern, als dass innerhalb der vom Betroffenen selbst bewohnten Wohnräumlichkeiten nach §463a Abs. 4 S. 1 2. HS StPO keine Datenerhebung stattfinden darf, bzw. diese nach S. 7 im Anschluss an die Erhebung unverwertbar zu machen ist.[350] Die von der JI-Richtlinie in ErwG 35 als demonstratives Beispiel gewählte Einwilligung in die Überwachung des Aufenthaltsortes mittels elektronischer Fußfessel ist also unter den tatsächlichen normativen Anforderungen des BDSG nicht mit einer Einwilligung datenschutzrechtlich legitimierbar, da zur Ermittlung der Freiwilligkeit die jeweiligen Umstände berücksichtigt werden müssen und mithin keine echte freie Entscheidung des Betroffenen angenommen werden kann.[351]

(2) Berücksichtigung der Umstände bei Einwilligungsabgabe

Die Umstandsermittlung nach §51 Abs. 4 S. 2 BDSG spielt grundsätzlich im Verhältnis Bürger zum Staat eine gewichtige Rolle. Trifft der Bürger auf die Polizei, so wird von diesem überwiegend ein hierarchisches Verhältnis angenommen.[352] Nicht zuletzt, weil die Polizei im Rahmen ihrer Aufgabenerfüllung das staatliche Gewaltmonopol besitzt und dieses etwa bei der Kriminalitätsbekämpfung auch konsequent durchsetzt. Beim Bürger führt dieser Umstand oft zu einer Primärassoziation, dass die Polizei in ihrer Aufgabenausübung unmittelbaren Zwang ausübt.[353] Dies

[349] Golla/Skobel, GSZ 2019, 140
[350] Coen in BeckOK StPO, §463a StPO Rn. 17
[351] Müller/Schwabenbauer in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 474
[352] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, §51 BDSG Rn. 27
[353] Ley, Polizei & Wissenschaft 1/2013, S. 58

resultiert nicht selten darin, dass Bürger der Annahme unterliegen polizeilichen Maßnahmen grundsätzlich Folge leisten zu müssen.[354]

Da polizeiliche Zwangsmaßnahmen im Ermittlungsverfahren gegenüber einem Betroffenen regelmäßig einen Eingriff in dessen Grundrechte bedeuten, findet sich dieser typischerweise in einer den Eingriff abwehrend wollenden Position wieder.[355] Dies folgt schon aus dem Umstand, dass zu dem Zeitpunkt, in dem der Betroffene selbst im Ermittlungsverfahren den Beschuldigtenstatus erhält, sich selbst also nun der Begehung eines Rechtsverstoßes ausgesetzt sieht.[356] Sind Betroffenen also Beschuldigungen entgegengebracht, so müssen diese damit rechnen, dass jede Handlung oder jedes Unterlassen auch eine Würdigung seitens der Polizei erfährt. In einer solchen Ausnahmesituation, auf welche die wenigsten Bürger vorbereitet sein dürften, ist demnach anzunehmen, dass ein Betroffener nachvollziehbar dem Glauben erliegen kann, es sein für ihn nachteilhaft, wenn er das Angebot eines Polizeibeamten ausschlagen würde.[357] Etwa weil die Polizei daraufhin das Verweigern als Schuldeingeständnis interpretieren könnte oder sogar eine Provokation weiterer polizeilicher Maßnahmen nach sich ziehen kann.[358] Für den Betroffenen dürfte die Situation zusätzlichen Stress verursachen, wenn die Situation aus einer direkten physischen oder fernmündlichen Konfrontation mit den Polizeibeamten hervorgeht.[359] Ist ein Betroffener also in einer Situation wo diese keine klare Abwägung treffen kann, weil er von falschen Umständen ausgeht, so wird dieser in der Folge auch nicht alle Fakten kennen, die er bräuchte um eine wirksame Einwilligung abzugeben.[360] Kann der Betroffene also nicht alle relevanten Aspekte zur Entscheidungshilfe heranziehen, muss angenommen werden, dass die Entscheidung Begründungsfehler enthält, welche bei voller Kenntnis der

[354] Mosbacher, NStZ 2015, 42
[355] Stellungnahme des ULD (Schleswig-Holstein) zur Novellierung der DNA-Analyse im Strafverfahren, https://www.datenschutzzentrum.de/artikel/167-Stellungnahme-des-ULD-zur-Novellierung-der-DNA-Analyse-im-Strafverfahren.html; abgerufen am 23.09.2023
[356] Kasiske, JuS 2014, 15
[357] Geppert, NStZ 2014, 481
[358] El-Gazhi, ZIS 2019, 110
[359] Aden in Rauch, Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, S. 10
[360] El-Ghazi, ZIS 2019, 116

Lage nicht oder zumindest deutlich weniger ausgeprägt aufgetreten wären.[361] Die Entscheidungsfindung zwischen möglichen Handlungsalternativen beruht nämlich gerade auf der Sammlung und Analyse aller situativ verfügbaren Informationen, um diese bewusst abwägen zu können und daraus resultierend die Entscheidung zu treffen.[362] Unterliegt ein Betroffener also wie erwähnt der Annahme, er sei grundsätzlich dazu verpflichtet eine polizeiliche Maßnahme zu erdulden, so wird dieser in seiner Entscheidungsfindung zum Resultat kommen, überhaupt keine Handlungsalternative zu haben. Dementsprechend wird er der Maßnahme zustimmen, da er sonst fürchten muss diese würde unter dem Einsatz von Gewalt gegenüber ihm durchgesetzt. Ist ein Beschuldigter zwar in Kenntnis der Tatsache, dass er ein Wahlrecht hat einer Maßnahme zuzustimmen oder sie abzulehnen, aber gleichzeitig im Glauben ist, die Verweigerung seiner Einwilligung würde zu seinen Ungunsten interpretiert und argumentativ seinen Beschuldigtenstatus unterfüttern, so liegt auch hier ein Mangel in der Entscheidungsfindung vor.[363] Nun ergeben sich zwar zwei Handlungsalternativen, diese stehen aber in einem Missverhältnis zueinander, so dass der Beschuldigte dazu geneigt ist der angebotenen Maßnahme zuzustimmen, um in die für ihn vermeintlich günstigere Ausgangssituation zu gelangen.[364] In voller Kenntnis der Sachlage wäre der Beschuldigte möglicherweise zu einer anderen Entscheidung gekommen,[365] gerade um sich nicht unnötigerweise selbst zu belasten.[366] Jedenfalls wäre die Entscheidungsfindung nicht dahingehend mangelhaft, dass diese nun annähernd gleichwertige Handlungsalternativen für den Beschuldigten aufzeigen könnte.[367]

[361] Bühler in Scheiderer, Human Factors im Cockpit, S.164
[362] Bühler in Scheiderer, Human Factors im Cockpit, S.145
[363] Schwichtenberg in Kühling/Buchner, DS-GVO BDSG, §51 BDSG Rn. 6
[364] El-Ghazi, ZIS 2019, 110
[365] Bühler in Scheiderer, Human Factors im Cockpit, S.165
[366] Kasiske, JuS 2014, 15
[367] Bühler in Scheiderer, Human Factors im Cockpit, S.164

(3) Informiertheit bei Einwilligungsabgabe

Schon nach der Legaldefinition der Einwilligung nach §46 Nr. 17 BDSG müssen Betroffene müssen dementsprechend ausreichend informiert sein, um einem ordentlichen Entscheidungsprozess hinsichtlich der Abgabe einer Einwilligung zu unterliegen. Fehlt es an relevanten Informationen so kann die Einwilligung nicht als wirksam erteilt angesehen werden.[368] Ferner darf es ebenfalls nicht zu einer Überinformation des Betroffenen kommen, also die Versorgung mit nicht notwendigen Informationen.[369] Der Betroffene darf nicht erst zwischen relevanten und irrelevanten Informationen unterscheiden müssen, da sonst wiederrum ein Risiko der falschen Entscheidungsfindung besteht, welches in einer unwirksamen Ausübung des Rechts auf informationelle Selbstbestimmung münden kann.[370] Folglich muss die Behörde für alle nach Maßgabe des §51 Abs. 1 BDSG einwilligungsfähigen Zwangsmaßnamen eine angemessene Informationsversorgung hinsichtlich der einzuwilligenden Verarbeitung personenbezogener Daten sicherstellen. Dazu gehört insbesondere auch die Kundgabe der verarbeitenden Behörde, die konkreten Arten von personenbezogenen Daten, die der Verarbeitung zugrunde liegen, sowie der Zweck,[371] für welchen die Daten konkret verwendet werden sollen.[372] Sollen mehrere Zwecke bedient werden, so sind diese auch allesamt transparent zu machen.[373]

Ist ein Betroffener über eine Verarbeitung ausreichend informiert, so hat dieser damit zumindest den sachlichen Hintergrund, welcher er für seinen Entscheidungsprozess benötigt. Weiter muss er aber durch die Polizeibehörde auch in Kenntnis gesetzt werden, dass die Bereitstellung seiner Daten derart freiwillig ist, dass sich dieser auch bei einer Verweigerung keinerlei staatlichen Repressionen ausgesetzt sieht.[374] Eine Inkenntnissetzung durch die Behörde kann dann entfallen, wenn der

[368] Schaar, ZD 2017, 213
[369] Raum in Ehmann/Selmayr, DS-GVO, Art. 89 DSGVO Rn. 34
[370] Schaar, ZD 2017, 213
[371] explizit erwähnt in §51 Abs. 4 S.3 BDSG
[372] vgl. §55 BDSG
[373] Buchner/Kühling in Kühling/Buchner, DS-GVO BDSG, Art. 7 DSGVO Rn. 59
[374] Frenzel in Paal/Pauly, DS-GVO BDSG, §51 BDSG Rn. 8

Betroffene bereits über das Ausbleiben negativer Konsequenzen informiert ist.[375] In diesem Fall ist dann allerdings die Tatsache der bereits bestehenden Informiertheit des Betroffenen durch die Behörde zu überprüfen. Es dürfen keine Zweifel daran bestehen, dass der Betroffene die Entscheidung zur Abgabe der Einwilligung ohne jeglichen Zwang erteilt hat.[376]

Ein solcher Zweifel ist im Verhältnis Bürger und Staat generell zu vermuten, insbesondere wenn dieser im Rahmen von Strafprozessen auftritt, da Beteiligte hierbei ins eine besondere Drucksituation gebracht werden, aus welcher heraus sie agieren müssen.[377] Strittig ist, ob hinsichtlich der Freiwilligkeit eine generelle Belehrungspflicht wegen einer möglichen Selbstbelastung besteht,[378] oder diese von der jeweiligen Maßnahme und dem Einzelfall abhängig ist.[379] So kann ein Belehrungsgebot hinsichtlich der Auswirkungen der Einwilligungsabgabe aber gerade deswegen angenommen werden, weil sonst der Zweifel am vermuteten Über-/Unterordnungsverhältnis zwischen Staat und Bürger nicht ausgeräumt werden kann.[380] Freilich lässt sich die datenschutzrechtliche Belehrung in der Praxis nur schwer von der Belehrung hinsichtlich des Rechts zur Verweigerung einer einwilligungsbedürftigen Maßnahme trennen. Der begründende Entscheidungswille basiert schließlich auf demselben Informationspool. Ein Streitentscheid ist damit nicht erforderlich, da sich allein aus der datenschutzrechtlichen Anforderung der Zurverfügungstellung aller notwendigen Informationen durch die verarbeitende Behörde eine solche Belehrung ergibt.[381]

---

[375] Johannes/Weinhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 48
[376] Schwichtenberg in Kühling/Buchner, DS-GVO BDSG, §51 BDSG Rn. 6
[377] Singelnstein, NStZ 2020, 639
[378] Geppert, NStZ 2014, 481; LG Freiburg, Urteil v. 21.09.2009 - 9 Ns 550 Js 11375/09 – AK 92/09; AG Freiburg, Urteil v. 23.10.2009 – 27 Cs 540 Js 18733/09 – AK 2279/09; AG Michelstadt, Urteil v. 22.11.2011 - 2 OWi 1400 Js 22301/11; AG Frankfurt a.M., Urteil v. 18.01.2010 - 998 OWi 2022-955 Js-OWi 20697/09
[379] Cierniak, NZV 2012, 409; KG, Beschluss v. 30.7.2014 − 3 Ws (B) 356/14 – 122 Ss 106/14; OLG Brandenburg − Beschluss v. 16.4.2013 – (2 B) 53 Ss-OWi 58/13 (55/13)
[380] Johannes/Weinhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 41
[381] El-Ghazi, ZIS 2019, 110

(4) Belehrung über die Folgen der Einwilligungsabgabe

Eine Belehrung hinsichtlich der Folgen der Einwilligungsversagung ist nach Maßgabe des BDSG jedoch nicht zwingend erforderlich. §51 Abs. 4 BDSG fordert eine solche immer nur nach einer vorherigen Erforderlichkeitsprüfung im Einzelfall oder auf Verlangen des Betroffenen selbst. Das Verlangen des Betroffenen selbst muss nicht zwingend durch ein ausdrückliches Ersuchen übermittelt werden, sondern kann ebenfalls konkludent erfolgen.[382] Das Verlangen kann sich hierbei auch nur auf einzelne Teile der Belehrung erstrecken, wenn der Betroffene dies ersucht.[383] Eine Entscheidung der Belehrung im Einzelfall, wie sie in Abs. 4 statuiert ist, dürfte aufgrund des festgestellten angenommenen Über-/Unterordnungsverhältnisses zwischen Staat und Bürger sowie der zu erwartenden Druck- bzw. Stresssituation des Betroffenen regelmäßig erforderlich sein.[384] Durch die behördliche Festsetzung eines knappen Zeitlimits zur Einwilligungsabgabe dürfte ebenfalls die Freiwilligkeit beeinträchtigt werden, da so der Druck noch zusätzlich erhöht wird und der Betroffene möglicherweise nicht ausreichend Bedenkzeit erhält.[385] Auch wenn für die Beamte ersichtlich ist, dass ein Betroffener unsicher wirkt, oder seine Mimik indikative Anzeichen erweckt, dass dieser nicht alle notwendigen Informationen besitzt, um entscheiden zu können, so kann eine umfängliche Belehrung erforderlich sein. Dies folgt schon allein aus der notwendigen situativen Betrachtungspflicht.[386] Nur wenn der Betroffene auch hinsichtlich der tatsächlichen Folgen einer Einwilligungsverweigerung aufgeklärt wurde, kann dieser tatsächlich freiwillig entscheiden.[387] Nicht zuletzt auch deswegen, weil das Kriterium der Informiertheit sich – mindestens aus einem Umkehrschluss heraus – auch auf Nichtkonsequenzen beziehen kann,[388] also die

[382] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 31
[383] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 31
[384] Johannes/Weinhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 48
[385] Golla, KriPoZ 2019, 238
[386] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 29
[387] Schwichtenberg in Kühling/Buchner, DS-GVO BDSG, §51 BDSG Rn. 6
[388] Arning/Rothkegel in Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 4 DSGVO Rn. 341

Information welche Folge gerade nicht eingeleitet wird, der Betroffene also keinem Irrtum unterliegt.[389]

(5) Dokumentation der Einwilligungsabgabe

Für die Behörde ergibt sich aus der Belehrung und der Einzelfallprüfung aber auch die Pflicht zur Dokumentation.[390] Die Nachweiserbringung des Vorliegens aller Wirksamkeitskriterien der Einwilligung obliegt folgend aus §51 Abs. 1 2. HS BDSG schließlich dem Verantwortlichen. Dieser unterliegt insofern einer Darlegungspflicht, als dass aus seiner Dokumentation hervorgehen muss, dass der Betroffene in Kenntnis aller relevanten Umstände war und diese auch verstanden hat, was eine damit verbundene Datenverarbeitung legitimiert.[391] Eine reine Tatsachendokumentation, dass eine Belehrung stattgefunden habe, ist dabei nicht ausreichend.[392] Eine inhaltliche Nachvollziehbarkeit der vollzogenen Belehrung muss gegeben sein.[393] Dabei gilt es auch für die Behörde wiederum genau das richtige Maß an Dokumentation zu führen.[394] Werden mehr Informationen als zur Darlegung der Abgabe einer freiwilligen Einwilligung notwendig gesammelt, so ist dies zur Zweckerreichung nicht erforderlich. Durch das aus §47 Nr. 3 BDSG abgeleitete Datenminimierungsgebot besteht zumindest für die übermäßig gesammelten Daten damit keine Rechtsgrundlage.[395]

Kann bei einer persönlichen Belehrung des Betroffenen durch die anwesenden Polizeibeamten noch dessen Verständnislage beurteilt werden, gestaltet sich dies bei elektronischen Einwilligungsersuchen deutlich schwieriger. Hier kann dem Betroffenen zwar jede sachdienliche Information zur Verfügung gestellt werden, dessen persönlicher Verarbeitungsprozess jedoch nicht nachvollzogen werden.[396] Jedoch

[389] BGH, Urteil v. 02.12.1963 - III ZR 222/62
[390] Johannes/Weinhold in Sydow/Marsch, DS-GVO | BDSG, §51 BDSG Rn. 26
[391] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 14
[392] AG Frankfurt, Urteil v. 18.01.2010 – 998 OWi 2022
[393] Artikel-29-Datenschutzgruppe, 17/DE WP 259 rev.01, S.24f, https://www.datenschutzstelle.li/application/files/3615/3674/7263/wp259rev01_de.pdf; abgerufen am 30.09.2023
[394] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, §51 BDSG Rn. 35
[395] Braun in Gola/Heckmann, DS-GVO BDSG, §47 BDSG Rn. 17
[396] EuGH (Zweite Kammer), Urteil v. 11.11.2020 – C-61/19

muss ein Betroffener auch in einer solch nicht direkt-konfrontativen Situation die Möglichkeit besitzen, Kontakt zur Polizeibehörde aufzunehmen, um etwaige Verständnisfragen zu stellen, bevor dieser seine Einwilligung abgibt.[397] Dies käme auch dem Wunsch einer Belehrung aus Abs. 4 gleich.[398] Vorgesehene Kommunikationskanäle sind dem Betroffenen hierfür auch mitzuteilen.[399]

(6) Abgabe der Einwilligung unter Einfluss von Betäubungsmitteln

Besonders bei durchgeführten polizeilichen Verkehrskontrollen nach §36 Abs. 5 StVO ist aber es nicht fernliegend, dass bei einer kontrollierten Person es zu physischen oder psychischen Auffälligkeiten kommt. Kontrollschwerpunkt stellt neben der Überprüfung des technischen Zustandes des Fahrzeuges[400] häufig auch genau eine Fahrtüchtigkeitsüberprüfung statt.[401] Gibt es bei einem Betroffenen Anhaltspunkte, dass dieser etwa unter Alkohol- oder Drogeneinfluss ein Fahrzeug führt, so kann diesem der Beschuldigtenstatus eröffnet werde und das strafprozessuale Ermittlungsverfahren eingeleitet werden.[402] Wird in der Folge nun allerdings seitens der Behörde eine einwilligungsfähige Maßnahme nicht angeordnet, sondern stattdessen die Einwilligung des Beschuldigten erbeten, so ist hierbei die Frage aufzustellen, inwieweit sich der Konsum von Rauschmitteln auf die Einwilligungsfähigkeit auswirken können.

Um einwilligungsfähig zu sein ist das Vorliegen der allgemeinen Geschäftsfähigkeit nach Verständnis des BGB[403] nach der Rechtsprechung nicht erforderlich, da die abzugebende Einwilligung nicht auf die Herbeiführung eines Rechtsgeschäfts abzielt.[404] Gleichfalls ist auch die im Strafverfahren relevante Schuldfähigkeit i.S.d. §20 StGB

[397] Paschke in Gola/Heckmann, DS-GVO BDSG, §55 BDSG Rn. 6
[398] Stemmer/Wolf in BeckOK DatenschutzR, §51 BDSG Rn. 31
[399] Klement in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 7 DSGVO Rn. 74
[400] Freymann in Geigel, Haftpflichtprozess, §36 StVO Rn. 728
[401] Hühnermann in Burmann/Heß/Hühnermann/Jahnke, Straßenverkehrsrecht, §36 StVO Rn. 12
[402] Weingarten in KK-StPO, §160 StPO Rn. 14
[403] Umkehrschluss aus der in §104 BGB statuierten „Geschäftsunfähigkeit“
[404] BGH, Urteil v. 22.01.1953 - 4 StR 373/52; BGH, Urteil v. 05.12.1958 - VI ZR 266/57

nicht für eine wirksame Einwilligungsabgabe erforderlich.[405] Vielmehr kommt es auf die individuelle Einsichts- und Beurteilungsfähigkeit an, die ein Betroffener in der der Einwilligungsabgabe gegenwärtigen Situation innehat.[406]

Auch der Konsum von Alkohol widerspricht der Einwilligungsfähigkeit nicht im Vorhinein.[407] Steht ein Betroffener unter dem Einfluss von Alkohol, so kann etwa beim Auftreten von deutlichen Ausfallerscheinungen darauf geschlossen werden, dass eine die Fähigkeit zur Abgabe einer wirksamen Einwilligung unabhängig vom tatsächlichen Promillewert der Blutalkoholkonzentration (BAK) nicht gegeben ist.[408] Sind keine oder nur geringe Ausfallerscheinungen ersichtlich, etwa ein lediglich leicht schwankender Gang, so gibt es jedenfalls dahingehend keine Anhaltspunkte an der Verstandesreife eines Betroffenen zu zweifeln.[409] Erst ab einem Wert von zwei Promille BAK liegt eine unmittelbare Vermutung einer nicht mehr ausreichenden Verstandsreife vor, so dass eine Einwilligung seitens der Behörden nicht mehr ersucht werden sollten.[410] Selbiges gilt ebenfalls, wenn der Betroffene einer Beeinflussung durch Drogen unterliegt. Auch diese führt analog zum Alkoholkonsum nicht unmittelbar zu einer Verneinung der Einwilligungsfähigkeit des Betroffenen.[411]

Die Einwilligungsfähigkeit ist demnach Bestandteil der Berücksichtigung der Gesamtumstände, da diese ebenfalls immer in der individuellen Situation beurteilt werden muss.[412]

(7) Abgabe der Einwilligung bei Täuschung

Im Rahmen der Gesamtbeurteilung gilt es auch eine etwaige durch die Polizeibehörden vorgenommene Täuschung des Betroffenen zu

[405] BGH, Urteil v. 14.08.1963 – 2 StR 181/63
[406] Paeffgen/Zabel NK-StGB, §228 StGB Rn. 14; BGH, Urteil v. 22.02.1978 - 2 StR 372/77
[407] LG Saarbrücken, Beschluss vom 13. 11. 2008 - 2 Qs 53/08
[408] OLG Hamm, Beschluss v. 02.11.2010 - 3 RVs 93/10
[409] OLG Hamm, Beschluss v. 28.04.2009 - 2 Ss 117/09
[410] OLG Hamm, Beschluss v. 02.11.2010 - 3 RVs 93/10
[411] Goers in BeckOK StPO, §81a StPO Rn. 16
[412] Paeffgen/Zabel in NK-StGB, §228 StGB Rn. 16

berücksichtigen. Wurde diesem durch einen Polizeibeamten wider besseren Wissens etwa unterbreitet, dass die Abgabe einer Blutprobe nur zur Bestimmung des Blutalkoholspiegels herangezogen wird, während tatsächlich auch eine Untersuchung auf andere Stoffe hin stattfindet oder diese für den Strafprozess überhaupt nicht von Bedeutung wäre, so wurden dem Betroffenen maßgebliche Informationen bezüglich der Datenverarbeitung vorenthalten.[413] Glaubt der Betroffene nun den Angaben des Polizeibeamten, so unterliegt dieser einer Täuschung und kann in der Folge nur eine unfreie und damit unwirksame Einwilligung abgeben, welche die Behörde nicht als Rechtsgrundlage für eine Datenverarbeitung heranziehen darf.[414] Gleichermaßen stellt es aber auch eine Täuschung dar, wenn dem Betroffenen durch die Abgabe der Einwilligung ein geringeres Strafmaß seitens der Polizei in Aussicht gestellt wird.[415] Solche Zugeständnisse überschreiten die polizeilichen Kompetenzen und können letztendlich nur von einem Richter aufgeworfen werden.[416] Entsprechendes gilt aber auch wenn seitens der Behörde eine Drohung gegenüber dem Betroffenen ausgesprochen wird, beispielsweise dass dieser mit verschärften Maßnahmen zu rechnen habe, wenn die Abgabe einer Einwilligung unterbleibt.[417] Auch dann kann der Betroffene nicht in freier Entscheidung einwilligen, was der Begründung einer dafür notwendigen Rechtsgrundlage zur Datenverarbeitung entgegen steht.[418] Auch eine etwaige zivilrechtliche Anfechtung nach §143 BGB ist damit für den Betroffenen obsolet, da erst gar keine Einwilligung zustande kam.[419] Der Rückgriff auf das BGB ist dabei ohnehin umstritten,[420] eine Streitvertiefung kann an dieser Stelle aber dahinstehen.

[413] Schuhr in MüKO-StPO, §136a StPO Rn. 44
[414] Schwabenbauer in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 57
[415] Der bloße Hinweis auf eine mögliche Strafmilderung ist nicht zu beanstanden: Volbert, R&P 2016, 34
[416] EGMR (V. Sektion), Entscheidung v. 23.11.2010 – 21698/06
[417] Stemmer/Wolff in BeckOK DatenschutzR, §51 BDSG Rn. 31
[418] Stemmer/Wolff in BeckOK DatenschutzR, §51 BDSG Rn. 31
[419] Klement in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 7 DSGVO Rn. 93
[420] Klement in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 7 DSGVO Rn. 83

f) Zwischenergebnis

Zentraler Punkt bleibt damit die individuelle Berücksichtigung der situativ relevanten Umstände, welche zur Beurteilung der Freiwilligkeit gesamtheitlich herangezogen werden müssen und im Zweifel von der Behörde auch nachzuweisen sind. Können die Zweifel nicht ausgeräumt werden, so kann keine Freiwilligkeit angenommen werden und die Einwilligung nicht wirksam abgegeben werden.

II. Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten

Nach §51 Abs. 5 BDSG muss eine abgegebene Einwilligung sich ausdrücklich auf personenbezogene Daten von besonderen Kategorien beziehen, insofern diese Gegenstand der vorzunehmenden Verarbeitung sein sollen. Eine Auflistung oder sonstige Definition von besonderen Kategorien personenbezogener Daten findet sich jedoch im BDSG nicht. Nach Art. 10 der JI-RL sind dies Daten, aus welchen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgeht. Weiter sind auch genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung unter die besonderen Kategorien zu fassen. Die Aufzählung der JI-RL entspricht damit auch dem Verständnis der DSGVO, welche in Art. 9 dieselben besonderen Kategorien anführt. Mithin kann zur Auslegung der besonderen Kategorien personenbezogener Daten auf die JI-RL zurückgegriffen werden.[421] Sollen durch die Behörde im Zuge der Maßnahme also Daten verarbeitet werden, welche einer der aufgeführten Kategorien entsprechen, so darf dies nach §48 Abs. 1 BDSG nur erfolgen, wenn dies unbedingt erforderlich ist. Die Erforderlichkeit schließt dabei etwa eine Vorratsspeicherung aus.[422] Für eine erforderliche

[421] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, §51 BDSG Rn. 46
[422] Müller in Lisken/Denninger, PolR-HdB, Kapitel G Rn. 816

einwilligungsbasierte Verarbeitung ist zusätzlich nach §51 Abs. 5 BDSG die ausdrückliche Einwilligung des Betroffenen erforderlich. Die Ausdrücklichkeit muss insofern bestehen, dass sie die Erklärung der Einwilligung auch exakt auf die besonderen Kategorien der zu verarbeitenden personenbezogenen Daten bezieht.[423] Der Betroffene muss dabei spezifisch auf die Besonderheit der Kategorien der zu verarbeitenden Daten hingewiesen werden und insbesondere über die Sensibilität der aus den Daten möglicherweise zu gewinnenden Informationen aufgeklärt werden.[424] Ein Schriftformerfordernis ergibt sich jedoch nicht aus der Ausdrücklichkeit.[425] Das Kriterium der Ausdrücklichkeit schließt dabei vor allem konkludente und mutmaßliche Einwilligungen aus, genau wie Einwilligungen, welche auf einem Stillschweigen der betroffenen Person basieren. Die Abgabe einer solchen ausdrücklichen Einwilligung ist demzufolge also an eine tatsächliche Willensäußerung geknüpft. Bezieht sich die Einwilligung aber noch auf andere Kategorien personenbezogener Daten, welche nicht den besonderen Kategorien zuzuordnen sind, so kann dieser Teil etwa auch weiterhin konkludent abgegeben werden.[426] Durch die Nachweispflicht des Verantwortlichen wird jedenfalls eine verschriftlichte Dokumentation der Einwilligung aber in jedem Falle wahrscheinlich.[427] Allerdings muss auch aus der Dokumentation klar hervorgehen, dass der Betroffene exakt in die Verarbeitung der ihm zuvor eröffneten besonderen Kategorien eingewilligt hat, bzw. sich dessen Einwilligung auch auf diese erstreckt.[428]

Sollen also besondere Kategorien von personenbezogenen Daten durch die Einwilligung eines Betroffenen verarbeitet werden, so gelten hierfür nochmals verschärfte Anforderungen. Dies betrifft zum einen die Ausdrücklichkeit der Einwilligung, welche vom Betroffenen abgegeben werden muss. Dieser muss zum anderen aber auch vorab speziell auf die

[423] Stemmer/Wolff in BeckOK DatenschutzR, §51 BDSG Rn. 32
[424] Frenzel in Paal/Pauly, DS-GVO BDSG, §51 BDSG Rn. 9
[425] Stemmer in BeckOK DatenschutzR, Art. 7 DSGVO Rn. 83
[426] Heckmann/Paschke in Gola/Heckmann, DS-GVO BDSG, §51 BDSG Rn. 46
[427] Stemmer in BeckOK DatenschutzR, Art. 7 DSGVO Rn. 83
[428] Stemmer in BeckOK DatenschutzR, Art. 7 DSGVO Rn. 83

zu erwartende Verarbeitung von besonderen Kategorien hingewiesen worden sein, damit die Tragweite seiner Entscheidung auch die potenzielle Sensibilität der zugrundeliegenden Daten erkennen lässt. Weiter ist für die Verarbeitung von besonderen Kategorien personenbezogener Daten auch die in §48 Abs. 2 BDSG vorgesehene Schaffung geeigneter Garantien zwingend.[429] Hierbei ist insbesondere die Konkretisierung des Grundsatzes der Sicherheit der Verarbeitung nach §47 Nr. 6 BDSG zu berücksichtigen.[430] Die konkrete Ausgestaltung und Nachweisbarkeit entsprechender Garantien obliegt aber immer einer Einzelfallprüfung durch die verarbeitende Stelle unter Ausübung des behördlich zugestanden pflichtmäßigen Ermessen.[431]

[429] Schwichtenberg in Kühling/Buchner, §48 BDSG Rn. 5
[430] Schwichtenberg in Kühling/Buchner, DS-GVO BDSG, §48 BDSG Rn. 6
[431] Braun in Gola/Heckmann, DS-GVO BDSG, §48 BDSG Rn. 14

G. Fazit

Die Verwendung der Rechtsgrundlage der Einwilligung zur Unterstützung polizeilicher Ermittlungen im Rahmen von Strafprozessen gestaltet sich als äußerst schwierig. Schon allein die durch §51 Abs. 1 BDSG notwendige Berücksichtigung der Einwilligung im Vorfeld durch den Gesetzgeber bei der Kodifizierung einzelner Vorschriften, beschränkt die tatsächliche Anwendung auf einen Bruchteil strafprozessualer Zwangsmaßnahmen. Bisherige Anwendungsfälle wie die in der Einleitung beschriebene Atemalkoholkontrolle im Rahmen einer Verkehrskontrolle scheiden mangels entsprechender einwilligungsermöglichender Vorschrift aus. Um eine breitflächigere Ermöglichung der Einwilligung zu forcieren, erfordert es also zunächst umfassender Nachbesserung an den zugrundeliegenden Vorschriften durch den Gesetzgeber. Aber auch die Einwilligung bei bereits bestehenden Rechtsvorschriften gestaltet sich schwierig. Da im Verhältnis Bürger und Staat regelmäßig ein Machtungleichgewicht unterstellt wird, müssen die einzelnen Einwilligungsvoraussetzungen sorgsam geprüft werden. Handelt ein Bürger unter der Annahme, dass dieser einer Maßnahme folgeleisten muss oder glaubt er auch nur, dass er bei Nichtbefolgung Nachteile erfährt, so liegt keine tatsächliche Freiwilligkeit mehr vor, welche zur Abgabe einer Einwilligung zwingend notwendig ist. Hierbei spielt auch durchaus die Befolgung des Informationsgebotes der Polizeibeamten in der jeweiligen Situation eine große Rolle. Diese müssen das Vorhaben der Einholung der Einwilligung auch gegenüber dem Betroffenen deutlich anzeigen, so dass diesem klar ist, dass er einer Wahlfreiheit unterliegt. Weiter muss dem Betroffenen ebenfalls bekannt sein, dass auch bei einer Versagung seiner Einwilligung diesem keine negativen Konsequenzen drohen. Die Zurverfügungstellung aller notwendigen Informationen obliegt dabei den Polizeibeamten. Diese müssen also in Kenntnis aller relevanten die Maßnahme betreffenden Informationen sein und diese dem Betroffenen auch verständlich vermitteln. Dabei obliegt es ihnen gleichermaßen auch sauber zu dokumentieren, dass der Betroffene in Kenntnis aller

Umstände war und gleichzeitig nicht dem Irrglauben einer Zwangsbefolgung der Maßnahme erlegen ist. Wie granular eine solche Dokumentation sein tatsächlich sein muss, lässt sich mangels Rechtsprechung nicht abschließend feststellen. Bedenkt man aber die Konsequenz, dass bei einem Nichtvorweisen der Einwilligung eine Datenverarbeitung ohne Rechtsgrundlage begründet würde, was einem Verstoß gegen den Grundsatz der informationellen Selbstbestimmung gleichkäme, so dürfte der Nachweis der Einwilligung keine reine bürokratische Formalie sein, sondern tatsächlich substanzieller Natur. Gerade der Staat als verpflichteter Bewahrer der Grundrechte seiner Bürger, darf sich hier nicht durch eine nicht stichhaltige oder interpretationsfähige Dokumentation des Einwilligungsnachweises angreifbar machen. Eine solche Dokumentation dürfte die Beamten im Regelfall bei der Durchführung einer Maßnahme zuverlässig ausbremsen, da sichergestellt werden muss, dass alle notwendigen Voraussetzungen für die Einholung der Einwilligung erbracht wurden und dies auch nachweisbar ist. Gleichzeitig muss dem Betroffenen auch noch in einer für diesen wahrnehmbaren Stress- oder Drucksituation klar gemacht werden, dass er in diesem Falle dem Ersuchen der Beamten nicht nachkommen muss. Erfolgt die Maßnahme aber in Zusammenhang mit anderen für den Betroffenen zumindest duldungspflichtigen Maßnahmen, so scheint es naheliegend, dass dieser nicht zwangsläufig zwischen den Maßnahmen differenzieren kann. Viel mehr bleibt es also immer jedem Einzelfall an sich geschuldet, das Vorliegen einer wirksamen Einwilligung tatsächlich anzunehmen und diese auch unmissverständlich nachweisen zu können. Selbst bei der theoretischen Annahme des Vorliegens aller notwendigen Einwilligungsbestandteile muss die verarbeitende Behörde auch immer noch die Grundsätze jeglicher Datenverarbeitungen einhalten. Das erfordert einerseits nicht nur im Vorhinein eine gründliche Vorbereitung jeglicher durch die Behörde mögliche Datenverarbeitung. Andererseits muss im Zweifel auch dem Betroffenen alle notwendigen Informationen hierüber zu teil werden, bevor dieser als umfassend informiert gilt. Möchte ein Betroffener also etwa Auskunft, über die von der Behörde getroffenen

eingesetzten technischen und organisatorischen Maßnahmen erhalten, so ist dies im Vorfeld einer Einwilligung durchaus legitim. Die Annahme, dass die Beamten allerdings hierüber umfassend Auskunft geben können erscheint aber praxisfern, was zu einer Problematik der ausreichenden Information führen kann.

Zusammengefasst lässt sich der tatsächliche Anwendungsfall der Einwilligung in strafprozessuale Maßnahmen wohl auf wenige Einzelfälle beschränken und bleibt größtenteils theoretischer Natur. Die Hürden an das Vorliegen einer wirksamen Einwilligung und deren Nachweis erscheinen in der Praxis zu hoch, die Rechtsgrundlage dadurch nicht sicher genug und die Gefahr einer staatlichen Grundrechtsverletzung ist eminent.

Literaturverzeichnis

Albrecht, Jan Philipp. *Das neue Datenschutzrecht der EU.* Baden-Baden: Nomos, 2016.

Auer-Reinsdorff, Astrid. *Handbuch IT- und Datenschutzrecht, 3. Auflg.* München: C.H.BECK, 2019.

Barthe, Christoph. *Karlsruher Kommentar zur Strafprozessordnung: StPO, 9. Auflage.* München: C.H.BECK, 2023.

Beukelmann, Stephan. „Die Unschuldsvermutung." *Neue Juristische Wochenzeitschrift Spezial*, 2016: 696.

Borges, Georg. *BeckOK IT-Recht, 11. Edition.* München: C.H.BECK, 2023.

—. *Cloud Computing: Rechtshandbuch.* München: C.H.BECK, 2016.

Brink, Stefan. *BeckOK Datenschutzrecht, 43. Edition.* München: C.H.Beck, 2021.

Burmann, Michael. *Straßenverkehrsrecht: Kommentar, 27. Auflage.* München: C.H.BECK, 2022.

Cierniak, Jürgen. „Pflicht zur Belehrung über die Freiwilligkeit der Teilnahme an einer Atemalkoholmessung?" *Neue Zeitschrift für Verkehrsrecht*, 2012: 409-413.

Denninger, Erhard. *Handbuch des Polizeirechts, 7. Auflage.* München: C.H.BECK, 2021.

Dürig, Günther. *Grundgesetz-Kommentar, 101. Auflage.* München: C.H.BECK, 2023.

Ehmann, Eugen. *Datenschutz-Grundverordnung: DS-GVO, 2. Auflg.* München: C.H.BECK, 2018.

Ehmmann, Eugen. „Registermodernisierung in Deutschland: Die Steuer-Identifikationsnummer als allgemeine Personenkennziffer." *Zeitschrift für Datenschutz*, 2021: 509-512.

El-Ghazi, Mohamad. „Die Einwilligug in strafprozessuale Zwangsmaßnahmen nach der Umsetzung der Richtlinie (EU) 2016/680 - das Ende der freiwilligen Atemalkoholkontrolle!" *Zeitschrift für Internationale Strafrechtsdogmatik*, 2019: 110-118.

Engeler, Malte. „Der Konflikt zwischen Datenmarkt und Datenschutz: Eine ökonomische Kritik der Einwilligung." *Neue Juristische Wochenzeitschrift*, 2022: 3398-3405.

Epping, Volker. *BeckOK Grundgesetz, 56. Edition.* München: C.H.BECK, 2023.

Fischinger, Philipp. „Der Grundrechtsverzicht." *Juristische Schulung*, 2007: 808-813.

Forgó, Nikolaus. *Betrieblicher Datenschutz: Rechtshandbuch, 3. Auflage.* München: C.H.BECK, 2019.

Geigel, Reinhart. *Der Hafrpflichtprozess, 28. Auflage.* München: C.H.BECK, 2020.

Geppert, Klaus. „Zur Belehrungspflicht über die Freiwilligkeit der Mitwirkung an einer Atemalkoholmessung und zu den Folgen ihrer Verletzung.“ *Neue Zeitschrift für Strafrecht*, 2014: 481-486.

Gola, Peter. *Datenschutz-Grundverordnung: DS-GVO, 2.Auflg.* München: C.H.BECK, 2018.

Golla, Sebastian. „Datenschutzrechtliche Schattengewächse in den Ländern – Herausforderungen bei der Umsetzung der JI-Richtlinie für die Polizei – .“ *Kriminalpolitische Zeitschrift*, 2019: 238-244.

—. „"Sie haben doch nichts zu verbergen?": Zur Möglichkeit einer Einwilligug in die Datenverarbeitung im Geltungsbereich der Richtlinie (EU) 2016/680.“ *Zeitschrift für das Gesamte Sicherheitsrecht*, 2019: 140-145.

Grabitz, Eberhard. *Das Recht der Europäischen Union: EUV/AEUV, 79. Auflage.* München: C.H.BECK, 2023.

Graf, Jürgen. *BeckOK StPO mit RiStBV und MiStra, 49. Edition.* München: C.H.BECK, 2023.

Graf, Jürgen-Peter. *Beck'scher Online-Kommentar OWiG, 13. Edition.* München: C.H.BECK, 2016.

Gusy, Christoph. „Polizeiliche Befragung am Beispiel des §9 PolG NRW.“ *Neue Zeitschrift für Verwaltungsrecht*, 1991: 614-620.

Hochmayr, Gudrun. „Elektronisch überwachter Hausarrest: Gegenwart und Zukunft in Deutschland und Österreich.“ *Neue Zeitschrift für Strafrecht*, 2013: 13-18.

Hoeren, Thomas. *Handbuch Multimedia-Recht, 57. Auflg,.* München: C.H.BECK, 2022.

Hofmann, Rainer. *Ausländerrecht, 3. Auflage.* Baden-Baden: Nomos, 2023.

Hornung, Gerrit. „Die Europäisierung des starfverfahrensrechtlichen Datenschutzes: Zum Anwendungsbereich der neuen Datenschutz-Richtlinie für Polizei und Justiz.“ *Zeitschrift für Internationale Strafrechtsdogmatik*, 2018: 566-574.

Hunold, Daniela. *Polizeiarbeit zwischen Praxishandeln und Rechtsordnung: Empirische Polizeiforschungen zur polizeipraktischen Ausgestaltung des Rechts.* Wiesbaden: Springer, 2020.

Jarass, Hans. *Charta der Grundrechte der Europäischen Union: GRCh, 4. Auflage.* München: C.H.BECK, 2021.

—. *Grundgesetz für die Bundesrepublik Deutschland: GG, 17. Auflage.* München: C.H.BECK, 2022.

Karg, Moritz. „Datenschutzrechtlicher Rahmen für "Device Fingerprinting": Das klammheimliche Ende der Anonyimität im Internet.“ *Zeitschrift für Datenschutz*, 2014: 285-290.

Kasiske, Peter. „Die Selbsbelastungsfreiheit im Strafprozess.“ *Juristische Schulung*, 2014: 15-20.

Kindhäuser, Urs. *Strafgesetzbuch-Kommentar: StGB, 6. Auflage.* Baden-Baden: Nomos, 2023.

Kipker, Dennis-Kenji. *Cybersecurity: Rechtshandbuch, 2. Auflage.* München: C.H.BECK, 2023.

—. *Recht der Informationssicherheit.* München: C.H.BECK, 2023.

Knauer, Christoph. *Münchener Kommentar zur Strafprozessordnung: StPO.* München: C.H.BECK, 2014.

Kühling, Jürgen. *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, 3. Auflg.* München: C.H.BECK, 2020.

Ley, Thomas. „Zum Verhältnis von Polizei zum Bürger - oder Kunden?“ *Polizei & Wissenschaft*, 2013: 57-70.

Mantz, Reto. *Handbuch Europäisches und deutsches Datenschutzrecht: Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor .* München: C.H.BECK, 2019.

Masing, Johannes. „Herausforderungen des Datenschutzes.“ *Neue Juristische Wochenzeitschrift*, 2012: 2305-2311.

Mosbacher, Andreas. „Keine Belehrungpflicht über Freiwilligkeit der Atemalkoholmessung: Praxiskommentar.“ *Neue Zeitschrift für Strafrecht*, 2015: 42-43.

Möstl, Markus. *BeckOK Polizei- und Sicherheitsrecht Bayern, 5. Edition.* München: C.H.BECK, 2017.

Müller, Eckhart. *Münchener Anwaltshandbuch Strafverteidigung, 3. Auflage.* München: C.H.BECK, 2022.

Paschke, Marian. *Hamburger Kommentar Gesamtes Medienrecht, 4. Auflage.* Baden-Baden: Nomos, 2020.

Sachs, Michael. *Grundgesetz-Kommentar: GG, 9. Auflage.* München: C.H.BECK, 2021.

Schaar, Katrin. „Anpassung von Einwilligungserklärungen für wissenschaftliche Forschungsprojekte: Die informierte Einwilligung nach der DS-GVO und den Ethikrichtlinien.“ *Zeitschrift für Datenschutz*, 2017: 213-220.

Schantz, Peter. *Das neue Datenschutzrecht: Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis.* München: C.H.BECK, 2017.

Scheiderer, Joachim. *Human Factors im Cockpit: Praxis sicheren Handelns für Piloten.* Heidelberg: Springer, 2011.

Schieder, Alfons. „Zur datenschutzrechtlichen Einwilligung in polizeiliche Zwangsmaßnahmen.“ *Zeitschrift für das gesamte Sicherheitsrecht*, 2021: 16-20.

Scholz, Rupert. „Strafbarkeit juristischer Personen?“ *Zeitschrift für Rechtspolitik*, 2000: 435-440.

Schwichtenberg, Simon. „Die "kleine Schwester" der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz.“ *Datenschutz und Datensicherheit*, 2016: 605-609.

Simitis, Spiros. *Datenschutzrecht: DSGVO mit BDSG.* Baden-Baden: Nomos, 2019.

Singelnstein, Tobias. „Folgen des neuen Datenschutzrechts für die Praxis des Strafverfahrens und die Beweisverbotslehre.“ *Neue Zeitschrift für Strafrecht*, 2020: 639-644.

Soiné, Michael. „Die strafprozessuale Online-Durchsuchung.“ *Neue Zeitschrift für Strafrecht*, 2018: 497-504.

Spindler, Gerald. *Recht der elektronischen Medien, 4. Auflage.* München: C.H.BECK, 2019.

Stief, Matthias. „Die Richtlinie (EU) 2016/680 zum Datenschutz in der Strafjustiz und die Zukunft der datenschutzrechtlichen Einwilligung.“ *Strafverteidiger*, 2017: 470-477.

Sydow, Gernot. *DS-GVO | BDSG Handkommentar, 3. Auflage.* Baden-Baden: Nomos, 2022.

Taeger, Jürgen. *DSGVO - BDSG - TTDSG, 4. Auflage.* Frankfurt a.M.: Fachmedien Recht und Wirtschaft, 2022.

Taupitz, Jochen. „Der rechtliche Status von Hirnorganoiden.“ *Medizinrecht*, 2021: 407-415.

Tinnefeld, Marie-Theres. „Die selbstbestimmte Einwilligung im europäischen Recht.“ *Zeitschrift für Datenschutz*, 2018: 391-398.

Volbert, Renate. „Falsche Geständnisse in polizeilichen Vernehmungen – Vernehmungsfehler oder immanente Gefahr?“ *Recht und Psychatrie*, 2016: 4-10.

Voßkuhle, Andreas. „Grudwissen - Öffentliches Recht: Der Grundrechtseingriff.“ *Juristische Schulung*, 2009: 313-315.

Wandtke, Artur-Axel. *Praxiskommentar Urheberrecht: UrhR, 6. Auflage.* München: C.H.BECK, 2022.

Weber, Klaus. *Rechtswörterbuch, 31. Edition.* München: C.H.BECK, 2023.

Eidesstattliche Erklärung

Erklärung:

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe; die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde nach meiner besten Kenntnis bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Berlin, den 30.10.23  Unterschrift

Zusammenfassung

Die Masterarbeit behandelt die Thematik der Verarbeitung von personenbezogenen Daten im Rahmen strafrechtlicher Ermittlungen, die aufgrund einer Einwilligung der betroffenen Person vorgenommen werden. Dabei werden die datenschutzrechtlichen Voraussetzungen analysiert, um festzustellen welche Vorgaben aus den zugrundeliegenden Datenschutzgesetzen beachtet werden müssen und wie diese umzusetzen sind. Hierbei wird sich maßgeblich auf das Bundesdatenschutzgesetz gestützt, welches die von der Europäischen Union erlassene JI-Richtlinie in Deutschland umsetzt. Dabei wird zunächst am Beispiel des Angebotes der Atemalkoholkontrolle durch die Polizei im Rahmen einer Verkehrskontrolle einführend die Praxisrelevanz der Frage dargestellt. Neben einer Darstellung der sich aus dem Bundesdatenschutzgesetz ergebenden Datenschutzgrundsätze und deren Ausprägung im Kontext der behördlichen Datenverarbeitung wird vor allem auf die speziellen Probleme der Einwilligung Bezug genommen. Hierbei zählt zum einen die Frage der Notwendigkeit des Vorliegens einer Rechtsvorschrift, welche die Einwilligung als legitime Verarbeitung bedenkt, womit derzeit nur wenige Vorschriften der Strafprozessordnung ausgestattet sind. Zum anderen wird das Verhältnis zwischen Staat und Bürger problematisiert, da die Durchführung einer polizeilichen Maßnahme für den Bürger immer eine Drucksituation bedeutet. Die Arbeit untersucht, inwiefern unter diesen Bedingungen die freiwillige Abgabe einer Einwilligung erfolgen kann und stellt dabei auch heraus, welche Informations- und Dokumentationspflichten seitens der verarbeitenden Behörde erbracht werden müssen. Die Thesis schließt mit dem Fazit, dass sich die Verarbeitung im Rahmen strafprozessualer Maßnahmen durch die Polizei auf einzelne Ausnahmefälle beschränkt. Die Hürden der Vornahme der Verarbeitung sind in der Praxis zu hoch, da die tatsächliche freiwillige Abgabe der Einwilligung des Betroffenen durch die Polizei nur schwer nachgewiesen werden kann und damit das Risiko einer staatlichen Datenverarbeitung ohne Rechtsgrundlage groß ist.