# EU-Datenschutzreform

## – das Ende der Einwilligung als Rechtsgrundlage für die polizeiliche Datenverarbeitung?

**Von PD Dirk Staack, Owschlag**[1]

Die EU-Datenschutzreform mit der Datenschutzgrundverordnung (DSGVO)[2] und der sog. JI-Richtlinie[3] wurden im April 2016 vom Europäischen Parlament und vom Rat der Europäischen Union verabschiedet.

Die Normen bilden den datenschutzrechtlichen Rahmen der Europäischen Union, sollen für eine Mindestharmonisierung des Datenschutzniveaus innerhalb der Europäischen Union sorgen und haben damit erhebliche Auswirkungen auf die Datenschutzregelungen in der Bundesrepublik. Nach einer Übergangszeit von zwei Jahren trat die DSGVO zum 25. Mai 2018 in Kraft und führte zu vielfältigen Diskussionen bei Behörden, Vereinen und Verbänden, Schulen, Firmen und auch bei Privatpersonen über die nunmehr zu beachtenden Datenschutzregelungen. In der öffentlichen Diskussion eher unbeachtet blieb die Verabschiedung der sog. JI-Richtlinie, die sich auf die Aufgabe der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten[4] oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit bezieht und sich damit insbesondere an die Polizei und die Justiz richtet. Die JI-Richtlinie musste bis zum 6. Mai 2018 in nationales Recht umgesetzt werden, so dass in zahlreichen Bundes- und Landesgesetzen Änderungsbedarf entstand.

Allerdings sind die Polizeigesetze noch nicht in allen Ländern entsprechend angepasst worden.[5] In diesem Zusammenhang wird diskutiert, ob die Einwilligung der betroffenen Person als Rechtsgrundlage polizeilicher Datenverarbeitung noch tragfähig ist.[6] Der vorliegende Beitrag soll daher am Beispiel des Landesrechts Schleswig-Holstein der Frage nachgehen, ob die Einwilligung in die polizeiliche Datenverarbeitung zum Zwecke der Strafverfolgung und der Gefahrenabwehr als Rechtsgrundlage durch die Umsetzung der JI-Richtlinie wegfallen wird bzw. bereits weggefallen ist.

## 1 Praxisrelevanz

Die Einwilligung in die Datenverarbeitung durch die betroffene Person ist für alle Felder polizeilicher Tätigkeit von Relevanz. Im Bereich der Strafverfolgung gibt es mehrere Befugnisnormen, die eine Einwilligung voraussetzen, z.B. § 81c StPO Untersuchung anderer Personen, § 81h StPO DNA-Reihenuntersuchung, § 81f StPO Verfahren bei molekulargenetische Untersuchung und § 81g StPO DNA-Identitätsfeststellung. Im präventiven Bereich regelt bereits die allgemeine Verfahrensvorschrift des § 177 LVwG, dass personenbezogene Daten zum Zwecke der Gefahrenabwehr verarbeitet werden dürfen, *„soweit dies durch Gesetz ausdrücklich zuglassen ist oder die betroffene Person eingewilligt hat.“* Daneben gibt es spezifische Regelungen, wie z.B. § 179 Abs. 4 LVwG Datenerhebung zur Gefahrenvorsorge und § 195 LVwG Datenabgleich. Zudem ist die Polizei häufig auf eine nicht normgebundene Einwilligung in die Datenverarbeitung angewiesen, z.B. im Rahmen der Zuverlässigkeitsüberprüfung bei Großveranstaltungen wie dem Wacken-Open-Air, die freiwillige Herausgabe von personenbezogenen Daten, die von der Identitätsfeststellung nicht umfasst sind und damit auf Basis der Eingriffsermächtigung nicht verlangt werden dürfen, wie die Handynummer oder die Erreichbarkeit auf der Arbeitsstelle oder die Erhebung von Vergleichsfingerabdrücken des Wohnungsinhabers nach einem Wohnungseinbruchsdiebstahl.[7]

## 2 Ausgangslage

Die DSGVO trat zum 25. Mai 2018 in Kraft und ist als europäische Verordnung unmittelbar geltendes Recht.[8] Sie enthält

*„Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten“*[9] und *„gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“*[10] Die DSGVO gilt jedoch u.a. nicht für *„die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“*.[11] Diese Formulierung entspricht dem Gegenstand und den Zielen der sog. JI-Richtlinie, die den *„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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“*[12]umfassen und damit besondere datenschutzrechtliche Anforderungen an die Polizei und die Justiz stellen. Für die polizeiliche Datenverarbeitung gehen demnach die strengeren Regelungen der JI-Richtlinie der DSGVO vor.[13]Über die Datenschutzgesetze des Bundes und der Länder sowie entsprechenden Anpassungen in zahlreichen Sicherheitsgesetzen wie der Strafprozessordnung und der Polizeigesetze entfaltet die JI-Richtlinie ihre Wirkung auch in den Datenverarbeitungsregelungen des polizeilichen Aufgabenvollzugs. Im Ergebnis sind in der Bundesrepublik eine Vielzahl von Bundesgesetzen und Landesgesetzen an den Vorgaben der JI-Richtlinie auszurichten. Der Bundesgesetzgeber hat bereits ein neues Bundesdatenschutzgesetz (BDSG)[14] und der Landesgesetzgeber Schleswig-Holstein ein neues Landesdatenschutzgesetz (LDSG-SH)[15] erlassen. Die erforderlichen Anpassungen der StPO und des LVwG stehen hingegen noch aus.

## 3 Anwendungsbereich der JI-Richtlinie

Der Anwendungsbereich der JI-Richtlinie ist aufgrund unterschiedlicher Aussagen in den Erwägungsgründen und dem eigentlichen Richtlinientext umstritten.[16] Nach Art. 1 der JI-Richtlinie richtet sich die Regelung an Behörden, die *„zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“* Daten verarbeiten. Damit sind zunächst Strafverfolgungsbehörden und die Justiz Adressat der Richtlinie. Im polizeilichen Aufgabenfeld ist die Richtlinie damit stets dann anzuwenden, wenn die Polizei Straftaten verfolgt und damit repressiv tätig wird. Umfasst ist allerdings auch die Verhütung von Straftaten und damit ein Aufgabenfeld, das klassisch der Gefahrenabwehr zuzurechnen ist. Die Erweiterung durch den Halbsatz *„einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“*[17] verdeutlicht diesen übergreifenden Ansatz, wobei sich die gefahrenabwehrende Datenverarbeitung an der Aufgabe der Strafverfolgung orientieren soll und nur diejenige Fälle erfasst, die im Zusammengang mit der Verfolgung einer Straftat stehen.[18] Nach den Erwägungsgründen zur JI-Richtlinie *„zählen dazu auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht“*, wie z.B. *„bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen“*.[19] Fraglich ist, unter welcher Regelung die polizeiliche Datenverarbeitung zur *„reinen“* Gefahrenabwehr, d.h. ohne Bezug zu einer Straftat fällt. Nach enger Auslegung der JI-Richtlinie wäre in solchen Fällen die DSGVO anzuwenden. Das Ziel, dass die polizeiliche Datenverarbeitung einheitlichen Regelungen folgt, wird dadurch jedoch verfehlt. Im Gegenteil, das Aufgabengebiet der Gefahrenabwehr würde je nach Tätigkeitsbereich der JI-Richtlinie oder der DSGVO unterfallen. Dies ist nach dem Erwägungsgrund Nr. 12 der JI-Richtlinie unproblematisch möglich, denn die Mitgliedstaaten können *„die zuständigen Behörden mit anderen Aufgaben betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt, als sie in den Anwendungsbereich des Unionsrechts fällt.“* Die Polizei wäre allerdings je nach Aufgabe unterschiedlichen EU-Vorgaben unterworfen, die der Gesetzgeber im jeweiligen Polizeigesetz zu berücksichtigen hat. Der schleswig-holsteinische Gesetzgeber hat diesen Umstand bei der Umsetzung der JI-Richtlinie in das LDSG-SH Rechnung getragen, indem er die strengeren datenschutzrechtlichen Vorgaben der JI-Richtlinie auch für die *„reine“* Gefahrenabwehr übernimmt. Damit ist die polizeiliche Datenverarbeitung in Schleswig-Holstein losgelöst von der jeweiligen Aufgabe einheitlichen Datenschutzregelungen unterworfen.

## 4 Vorgaben der JI-Richtlinie hinsichtlich der Datenverarbeitung

Zur Frage der Einwilligung als Rechtsgrundlage für die Datenverarbeitung macht die JI-Richtlinie selbst keine Vorgaben, sondern gibt den Mitgliedstaaten nur auf, vorzusehen, dass *„die Verarbeitung nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Artikel 1 Absatz 1 genannten Zwecken wahrgenommenen wird, und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt.“*[20]Damit ist die Einwilligung als Rechtsgrundlage weder ausdrücklich vorgesehen noch ausgeschlossen. Hinweise

ergeben sich allein aus den 107 Erwägungsgründen, die das Europäische Parlament und der Rat den Normen der JI-Richtlinie vorangestellt haben. Zur Zulässigkeit der Datenverarbeitung auf Grundlage einer Einwilligung gibt es in den Erwägungsgründen zwei Fundstellen. Im Erwägungsgrund Nr. 35 der JI-Richtlinie sollte in Fällen, in denen die Person zur Verfolgung oder Verhütung einer Straftat aufgefordert wird, eine rechtliche Verpflichtung nachzukommen, die Einwilligung der betroffenen Person aufgrund der fehlenden Wahlfreiheit keine rechtliche Grundlage für die Verarbeitung von personenbezogenen Daten durch die zuständige Behörde darstellen. Im Umkehrschluss ist eine Einwilligung außerhalb solcher Verpflichtungen nicht ausgeschlossen, wie z.B. bei der Verarbeitung von Daten zur Gefahrenabwehr ohne Bezug zu Straftaten oder die Einwilligung in die Verarbeitung von Vergleichsfingerabdrücken des Wohnungsinhabers nach einem Wohnungseinbruchsdiebstahl. Darüber hinaus verweist der Erwägungsgrund im Weiteren auf die Zulässigkeit von Rechtsvorschriften, die vorsehen, dass die betroffene Person der Datenverarbeitung zustimmen kann und nennt das Beispiel der DNA-Analyse. Der Begriff *„Zustimmung“* ist hier als Sonderfall der Einwilligung zu sehen, bei dem trotz gesetzlicher Befugnis zur Datenverarbeitung eine Zustimmung der betroffenen Person erforderlich ist. Die „*Einwilligung*“ als nicht normgebundene Einwilligung in die Datenverarbeitung ist damit jedoch weiterhin in allen Fällen zulässig, in denen die betroffene Person keiner rechtlichen Verpflichtung unterliegt und damit eine echte Wahlfreiheit besteht. Diese Auslegung wird auch durch den Erwägungsgrund 37 der JI-Richtlinie gestützt. Dieser stellt klar, dass die Einwilligung in die Verarbeitung sensibler Daten, die besonders stark in die Privatsphäre der betroffenen Person eingreift, nicht möglich sein sollte. Im Umkehrschluss kann die Einwilligung ohne Bezug zu derartig sensiblen Daten grundsätzlich eine rechtliche Grundlage für die Datenverarbeitung darstellen, denn sonst wäre die Einschränkung bezogen auf die Einwilligung im Zusammenhang mit der Verarbeitung besonders sensible Daten unnötig. Die Auslegung, dass bereits der Erwägungsgrund Nr. 35 der JI-Richtlinie jegliche Einwilligung der betroffenen Person in die Verarbeitung personenbezogener Daten unmöglich macht, ist mit den Ausführungen zu besonders sensiblen Daten im Erwägungsgrund Nr. 37 der JI-Richtlinie demnach nicht in Einklang zu bringen.

Im Ergebnis sollte nach den Erwägungsgründen Nr. 35 und 37 der JI-Richtlinie eine Einwilligung zur Datenverarbeitung nicht ausreichen,

> wenn es aufgrund einer rechtlichen Verpflichtung im Rahmen der Verhütung und Verfolgung von Straftaten keine Wahlfreiheit gibt oder
>
> im Rahmen der Verhütung und Verfolgung von Straftaten besonders sensible Daten verarbeitet werden sollen.

In allen anderen Fällen ist eine Einwilligung in die Datenverarbeitung als Rechtsgrundlage nicht ausgeschlossen. Das gilt insbesondere für polizeiliche Datenverarbeitung zur *„reinen“* Gefahrenabwehr, die von der JI-Richtlinie eigentlich nicht erfasst wird. Unberührt bleibt zudem die Möglichkeit der Zustimmung zur Datenverarbeitung, soweit die Datenverarbeitung auf Grundlage einer ausdrücklichen gesetzlichen Regelung erfolgt.

## 5 Umsetzung der JI-Richtlinie durch das LDSG-SH

Das LDSG-SH wurde durch das *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680* vom 2. Mai 2018 angepasst.[21] Im Hinblick auf die o.g. Problematik der drohenden uneinheitlichen Regelungen zur Datenverarbeitung durch die Polizei bestimmt das LDSG-SH in § 20 (Anwendungsbereich), dass der Abschnitt zur Umsetzung der JI-Richtlinie *„den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten zuständigen öffentlichen Stellen“* mit einschließt.Damit ist die Datenverarbeitung der Vollzugspolizei sowohl zur Strafverfolgung als auch zur Gefahrenabwehr umfasst und zugleich die nicht-polizeiliche Gefahrenabwehr durch Verwaltungsbehörden ausgenommen. Für sie gilt grundsätzlich die DSGVO. Bezogen auf die Einwilligung als Rechtsgrundlage für die polizeiliche Datenverarbeitung enthält das LDSG-SH ebenfalls keine Regelung. Die bisher in § 11 LDSG-SH (a.F.)[22] enthaltene Regelung zur Zulässigkeit der Datenverarbeitung, die u.a. auch einen Einwilligungstatbestand enthielt, wurde durch eine allgemeine Regelung zur Zulässigkeit der Verarbeitung personenbezogenen Daten in den §§ 3, 23 LDSG-SH ersetzt. In der Neuregelung heißt es nur noch: *„Die Verarbeitung personenbezogener Daten ist zulässig, wenn sie für die Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.“* Nach der Gesetzesbegründung zu § 3 LDSG-SH wurde mit dieser Norm *„eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen geschaffen“.*[23]Die Regelung zur Einwilligung aus § 27 LDSG-SH normiert laut Gesetzesbegründung die *„Voraussetzungen für eine wirksame Einwilligung“*[24] und nicht die Frage, ob die Einwilligung Rechtsgrundlage einer polizeilichen Datenverarbeitung darstellen kann. Das Vorhandensein dieser Regelung im Abschnitt 3 des LDSG-SH spricht ebenfalls dafür, dass auch der Gesetzgeber von einer Rechtfertigung einer Datenverarbeitung durch Einwilligung ausgeht. § 27 Abs. 1 LDSG-SH normiert lediglich eine Nachweispflicht für die Polizei, soweit die Verarbeitung personenbezogener Daten auf Grundlage einer Rechtsvorschrift, welche die Einwilligung der betroffenen Person vorsieht, erfolgt. Hieraus im Umkehrschluss zu folgern, dass eine Einwilligung nur noch bei vorhandener Rechtsvorschrift, welche die

Einwilligung ausdrücklich vorsieht, in Betracht kommt, geht fehl. Die Erwägungsgründe zur JI-Richtlinie unterscheiden deutlich zwischen der Einwilligung und der Zustimmung zu einer Datenverarbeitung nach einer Rechtsnorm. Nachdem der Gesetzgeber offensichtlich darauf verzichtet hat, sowohl die Zulässigkeit der Datenverarbeitung durch Einwilligung in § 23 LDSG-SH zu regeln als auch die Unterscheidung zwischen Einwilligung und Zustimmung vorzunehmen, ist davon auszugehen, dass die Klärung dieser Fragen der Neuregelung des LVwG und weiteren Gesetzen vorbehalten ist, die als speziellere Normen den allgemeinen Regelungen des LDSG-SH vorgehen.

## 6 Novellierung der Polizeigesetze

Neben der aktuellen sicherheitspolitischen Diskussion zur Bedrohung durch den islamistischen Terrorismus hat auch die notwendige und mittlerweile zeitkritische Umsetzung der EU-Datenschutzreform zu umfassenden Novellierungsvorhaben bei Bund und Ländern geführt. Zugleich soll ein Musterpolizeigesetz die Harmonisierung der Polizeigesetze fördern, um ein einheitliches Sicherheitsniveau in Deutschland und eine gleichförmige Anwendung von gefahrenabwehrrechtlichen Befugnissen sowie datenschutzrechtlichen Vorgaben zu erreichen.[25] Die derzeitige Prüfung des Novellierungsbedarfs des letztmalig im Jahr 2007 überarbeiteten schleswig-holsteinischen LVwG umfasst daher auch die erforderlichen Anpassungen aufgrund der EU-Datenschutzreform. Bezogen auf die Einwilligung zeigen bereits überarbeitete Polizeigesetze, dass an der Möglichkeit der Einwilligung als Rechtsgrundlage für die polizeiliche Datenverarbeitung festgehalten wird.[26]

## 7 Fazit

Die Einwilligung als Rechtsgrundlage für die polizeiliche Datenverarbeitung zur Strafverfolgung und zur Gefahrenabwehr ist durch die EU-Datenschutzreform keinesfalls abgeschafft, vielmehr gibt es je nach Umsetzung der JI-Richtlinie in die nationalen Gesetze unterschiedliche Voraussetzungen für eine wirksame Einwilligung. Die Gesetzgeber sind aufgefordert, den Gestaltungsspielraum nach der EU-Datenschutzreform zu erkennen und normenklare Befugnisse für die polizeiliche Datenverarbeitung zu schaffen. Die Gesetzgeber schießen über die Idee der Einführung eines Mindeststandards bei der Datenverarbeitung innerhalb der EU hinaus, wenn sie die Grundrechtsträger durch eine zu enge Auslegung der EU-Datenschutzreform entmündigen, im Einzelfall über die Preisgabe ihrer persönlichen Daten informiert und selbstbestimmt zu entscheiden.

## Anmerkungen

1. Dirk Staack ist Polizeidirektor und Angehöriger des LKA Schleswig-Holstein. Er ist Herausgeber und Autoren von zahlreichen Fachpublikationen sowie Lehrbeauftragter im Masterstudiengang „Public Administration – Police Management“. Der Beitrag berücksichtigt die Gesetzgebungsverfahren bis zum 28.2.2019.
2. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 (DSGVO), Amtsblatt der Europäischen Union L 119/1.
3. Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 (JI-Richtlinie), Amtsblatt der Europäischen Union L 119/89.
4. Den Straftaten im Sinne der JI-Richtlinie dürften auch Ordnungswidrigkeiten zuzurechnen sein. Vgl. Schwabenbauer, in: Bäcker/Denninger/Graulich, 2018, Handbuch des Polizeirechts, 6. Auflage, S. 881 m.w.N. und LT-Drs. SH 19/429, S. 151.
5. Vgl. Schenke/Graulich/Ruthig, 2019, Sicherheitsrecht des Bundes, S. 7.
6. Vgl. Petri, in: Bäcker/Denninger/Graulich, 2018, a.a.O., S. 924 und LT-Drs. SH 19/752, S. 17.
7. Vgl. Becker/Brüning, 2014, Öffentliches Recht in Schleswig-Holstein, S. 188.
8. Vgl. Art. 99 DSGVO und § 1 BDSG.
9. Vgl. Art. 1 Abs. 1 Verordnung (EU) 2016/679 (DSVGO).
10. Vgl. Art. 2 Abs. 1 Verordnung (EU) 2016/679 (DSVGO).
11. Vgl. Art. 2 Abs. 2d Verordnung (EU) 2016/679 (DSVGO).
12. Vgl. Art. 1 Richtlinie (EU) 2016/680 (JI-Richtlinie).
13. Vgl. Kugelmann, 2018, Die Anpassung der Fachgesetze an die DS-GVO, DUD, S. 482; Schwabenbauer, in: Bäcker/Denninger/Graulich, 2018, a.a.O., S. 872.

14. BGBl 2017 I, S. 2097.
15. GVOBl SH 2018, S. 162.
16. Vgl. Schwabenbauer, in: Bäcker/Denninger/Graulich, 2018, a.a.O., S. 873; Kugelmann, 2018, a.a.O., DUD, S. 482.
17. Vgl. Art. 1 Richtlinie (EU) 2016/680 (JI-Richtlinie).
18. Vgl. Schwabenbauer, in: Bäcker/Denninger/Graulich, 2018, a.a.O., S. 882.
19. Richtlinie (EU) 2016/680 (JI-Richtlinie), Erwägungsgrund 12.
20. Vgl. Art. 8 Abs. 1 Richtlinie (EU) 2016/680 (JI-Richtlinie).
21. GVOBl SH 2018, S. 162.
22. GVOBl SH 2000, S. 169.
23. Vgl. LT-Drs. SH 19/429, S. 132.
24. Vgl. LT-Drs. SH 19/429, S. 152.
25. Vgl. Staack, 2018, Die Kriminalpolizei, Heft 3, S. 9.
26. Vgl. z.B. § 9 PolG NRW, Art. 31 BayPAG, § 32 TH PAG und § 39 Abs. 3 i.V.m. § 9 Abs. 3 BKAG.