Datenschutzrechtliche Schattengewächse in den Ländern – Herausforderungen bei der Umsetzung der JI-Richtlinie für die Polizei –

*von Dr. Sebastian J. Golla**

Abstract
Dieser Beitrag untersucht die Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (JIRL) durch die neuen Polizei- und Datenschutzgesetze der Länder. Er gibt einen kurzen Überblick über die abgeschlossenen und laufenden Verfahren hierzu und untersucht einige Problemschwerpunkte bei der Umsetzung. Defizite weisen die Regelungen zur Einwilligung, den Ausnahmen von Betroffenenrechten sowie zu den Befugnissen der Datenschutzaufsicht auf.

This article examines the implementation of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (JIRL) through the new police laws and data protection laws in the German federal Länder. It provides a short overview of the completed and ongoing proceedings and analyzes several key problems that occurred in the implementation process. Deficits become apparent in the rules about consent to data processing, the exceptions from individual rights and the competences of data protection authorities.

I. Polizeilicher Datenschutz im Wandel

Der Umgang mit personenbezogenen Daten ist das tägliche Brot der Polizei. Er erfuhr in den 1980er- und 1990er-Jahren infolge des Volkszählungsurteils des *BVerfG*[1] erstmals eine ausführliche gesetzliche Normierung. Aktuell befinden sich die betreffenden Regelungen im Umbruch. Eine wesentliche Ursache hierfür ist die Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (JIRL).[2] Sie macht umfassende Vorgaben für die Verarbeitung von personenbezogenen Daten 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, durch die hierfür zuständigen Behörden (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 JIRL). Damit erfasst die JIRL unter anderem die polizeiliche Datenverarbeitung zu präventiven und repressiven Zwecken.[3] Dies legt auch ErwGr 12 S. 1 JIRL nahe, nach dem die Tätigkeiten der Polizei „hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet" sind, auch wenn „nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht."

Die Umsetzung der JIRL hat damit eine potentiell hohe Relevanz für die polizeiliche Praxis. Dennoch findet sie momentan verhältnismäßig wenig Beachtung in der Öffentlichkeit und Fachkreisen. Dies liegt auch daran, dass die Umsetzung der JIRL gleich doppelt im Schatten steht: Zum einen ist die JIRL neben der gleichzeitig verabschiedeten Verordnung (EU) 2016/679 (DSGVO) der weniger beachtete Part der europäischen Datenschutzreform.[4] So wird die JIRL auch als „kleine Schwester"[5] der DSGVO bezeichnet. Die mit hohen Bußgeldandrohungen und einer unmittelbaren Geltung ausgestattete DSGVO erhielt besonders zu ihrem Geltungsbeginn massive öffentliche Aufmerksamkeit, wenn auch diese zum Teil von unpräzisen Informationen begleitet war. Die JIRL hingegen spielte in der Berichterstattung kaum eine Rolle und wurde teilweise auch mit der DSGVO verwechselt.[6]

Der zweite Schatten, der sich über die Umsetzung der JIRL gelegt hat, sind die hiervon unabhängig laufenden Reformen der Polizeigesetze der Länder. Die hier eingeführten oder diskutierten Änderungen sind äußerst grundrechtssensibel und ungleich öffentlichkeitswirksamer als die von der JIRL vorgesehenen Änderungen. Es ist kein Wunder, dass etwa die Einführung neuer Befugnisse zur Quellen-Telekommunikationsüberwachung und Online-Durchsuchung, die stärkere Bewaffnung der Polizei sowie die Präventivhaft für Gefährder mehr Aufmerksamkeit er-

* Der *Verfasser* ist wissenschaftlicher Mitarbeiter an der Johannes Gutenberg-Universität Mainz.

1 BVerfGE 65, 1.

2 Eine weitere Triebkraft der aktuellen Reformen der Regelungen zum polizeilichen Datenschutz ist das Urteil des *BVerfG* zum BKAG; BVerfGE 141, 220. Allerdings ist insbesondere zweifelhaft, inwiefern dieses eine Umstellung der polizeilichen Informationsordnung erfordert.

3 Nicht von der JIRL erfasst erscheint hingegen die sonderordnungsbehördliche Gefahrenabwehr. Der Zusatz „einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit" lässt sich so verstehen, dass Datenverarbeitungen zu diesen Zwecken nur dann vom Anwendungsbereich der JIRL erfasst sind, wenn ein Bezug zu den zuvor genannten „Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung" besteht; vgl. *Bäcker*, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, S. 63 (66 f.); *Hornung/Schindler/Schneider*, ZIS 2018, 566 (572); *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. (2018), Kap. G Rn. 376.

4 Vgl. *Aden,* vorgänge 2018, 93 (94); *Bäcker*, in: Hill/Kugelmann/Martini, S. 63 f.; *Hornung/Schindler/Schneider*, ZIS 2018, 566.

5 *Schwichtenberg*, DuD 2016, 605.

6 Vgl. etwa http://www.bpb.de/politik/hintergrund-aktuell/269454/neue-polizeigesetze (zuletzt abgerufen am 14.5.2019).

regen als die von der JIRL vorgesehenen Vorgaben an Datenstrukturen und Betroffenenrechte. Zumindest unglücklich ist aber, dass die Umsetzung der JIRL bei einer Umsetzung gleichzeitig mit diesen Reformen zum unbeachteten Annex gerät.

II. Stand der Umsetzung der JIRL

Die JIRL war zum 6. Mai 2018 umzusetzen. Allerdings haben im Frühjahr 2019 nur etwa die Hälfte aller Bundesländer[7] die Umsetzung der JIRL aus ihrer Sicht vollständig abgeschlossen. Aus manchen Ländern sind hingegen noch keinerlei konkrete Entwürfe zur Umsetzung der JIRL (öffentlich) bekannt – so etwa aus Bremen und dem Saarland. Soweit die Umsetzung bereits erfolgt oder konkret angegangen ist, lassen sich unterschiedliche gesetzgeberische Ansätze nachvollziehen. Einige Länder haben die Umsetzung der JIRL zunächst im Wesentlichen in den allgemeinen Datenschutzgesetzen geplant bzw. vollzogen.[8] Andere Länder nehmen die Umsetzung über spezielle Fachgesetze bzw. eigene JIRL-Gesetze in Angriff.[9]

Mit Blick auf den polizeilichen Bereich haben die unterschiedlichen Ansätze verschiedene Vor- und Nachteile. Soweit die Umsetzung der JIRL im Wesentlichen in den allgemeinen Datenschutzgesetzen erfolgt, werden diese neben den Polizeigesetzen heranzuziehen sein, wenn es um die Verarbeitung personenbezogener Daten geht. Die Polizeigesetze werden in diesen Fällen regelmäßig Verweise auf die allgemeinen Datenschutzgesetze enthalten. Der polizeiliche Anwender muss in diesem Fall also mit zwei Gesetzen nebeneinander arbeiten. Für den Gesetzgeber besteht gleichzeitig die Herausforderung, die Schnittstellen zwischen dem allgemeinen Polizeirecht und dem Datenschutzrecht sauber auszugestalten.

Ähnliches ergibt sich, soweit die Umsetzung in speziellen „JIRL-Gesetzen" erfolgt, die die Umsetzung der JIRL nicht in einem Zug mit der Nutzung von Spielräumen der DSGVO regeln. Zwar begünstigt diese Form der Umsetzung eine gründliche und konsistente Umsetzung der Vorgaben der JIRL, da die Gefahr geringer ist, dass diese mit Regelungen zur Nutzung der Spielräume der DSGVO vermengt werden. Auch hier wird der Anwender aber in der Regel zusätzlich spezielle Fachgesetze zu Rate ziehen müssen. Ein dritter Weg der Regelung wäre, die Umsetzung der JIRL (fast) ausschließlich in den Fachgesetzen vorzunehmen. Dies könnte allerdings zu einem massiven Anwachsen dieser Gesetze führen. Soweit ersichtlich hat sich kein Bundesland für letzteren Weg der Umsetzung entschieden.

III. Ausgewählte Probleme der Umsetzung

Im Folgenden betrachtet der Beitrag einige zentrale Probleme bei der Umsetzung der JIRL für den polizeilichen Bereich im Landesrecht.[10] Die Gesetzgebungsverfahren in den Ländern offenbaren hier unterschiedliche Probleme, teils aber auch Gemeinsamkeiten. Die folgenden Ausführungen sind nicht abschließend, sondern beziehen sich auf drei zentrale „Baustellen" bei der Umsetzung der JIRL, die in gleich mehreren Ländern Schwierigkeiten bereiteten.

1. Die Einwilligung als Verarbeitungsgrund

Probleme werfen zunächst jene Vorschriften der Gesetze zur Umsetzung der JIRL auf, die die Einwilligung der betroffenen Person als Rechtsgrundlage einer Datenverarbeitung im polizeilichen Bereich vorsehen.[11]

a) Das Grundproblem der Freiwilligkeit

Die Einwilligung ist als Rechtsgrundlage für die Datenverarbeitung im polizeilichen Bereich grundsätzlich problematisch. Dies beruht auf ihrer Voraussetzung der Freiwilligkeit. Die Einwilligung ist Ausdruck der informationellen Selbstbestimmung des Betroffenen.[12] Wird eine Person jedoch mit behördlichen Maßnahmen zur Strafverfolgung, Kriminalprävention oder Gefahrenabwehr konfrontiert, befindet sie sich regelmäßig in einer Drucksituation. Sie muss damit rechnen, dass sie, wenn sie nicht in eine Datenverarbeitung einwilligt, zu deren Duldung oder aktiver Mitwirkung verpflichtet wird und ihr durch die Weigerung Nachteile drohen. Das Verhältnis zwischen Polizei und Bürger ist nicht von freien Entscheidungsspielräumen und einvernehmlichem Handeln, sondern einseitiger Hoheitsausübung geprägt.[13]

Dem Umstand, dass die Freiwilligkeit der Einwilligung gegenüber öffentlichen Stellen besonders problematisch ist, trägt auch die – für die Polizei weitestgehend nicht anwendbare[14] – DSGVO Rechnung. Nach ErwGr 43 DSGVO ist die Einwilligung keine gültige Rechtsgrundlage, wenn sie gegenüber einer Behörde abgegeben wird und es deshalb in Anbetracht aller Umstände des konkreten Falls unwahrscheinlich ist, dass sie freiwillig erteilt wurde. Die Möglichkeit einer Einwilligung birgt auch das Risiko, dass Behörden die Voraussetzungen, die Ermächtigungsgrundlagen an eine Datenverarbeitung stellen, umgehen oder Maßnahmen ergreifen, die gesetzlich gerade nicht vorgesehen sind.[15] Damit verbunden ist die Gefahr, dass Behörden ihre Machtposition gegenüber dem Bürger nutzen, um eine Einwilligung zu erlangen, auch wenn diese nur unter Zwang abgegeben wird. Dieses Miss-

---

7 Bayern, Berlin, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Schleswig-Holstein und Thüringen.

8 Bayern, Berlin, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Schleswig-Holstein und Thüringen.

9 Baden-Württemberg, Brandenburg, Bremen, Hamburg, Saarland, Sachsen und Sachsen-Anhalt.

10 Vgl. vorwiegend zu der Umsetzung der JIRL im BDSG *Aden*, vorgänge 2018, 93 (98 ff.).

11 Dazu ausführlich *Golla/Skobel*, GSZ 2019 (im Erscheinen).

12 *Geiger*, NVwZ 1989, 35 (37); *Ingold,* in: Sydow, DSGVO, 2. Aufl. (2018), Art. 7 Rn. 40.

13 *Eßer*, in: Auernhammer, DSGVO/BDSG, 6. Aufl. (2018), Art. 4 DSGVO Rn. 98; *Aden,* vorgänge 2018, 93.

14 Vgl. Art. 2 Abs. 2 lit. c DSGVO.

15 *Stief,* StV 2017, 470 (470 f.).

brauchspotential spricht dafür, dass eine gegenüber Polizei und Strafjustiz erteilte Einwilligung in vielen Fällen nicht als freiwillig anzusehen ist.

b) Vorgaben der JIRL

Die beschriebene Problematik kommt auch in der JIRL zum Ausdruck. Diese nennt die Einwilligung in ihrem verfügenden Teil nicht als möglichen Erlaubnistatbestand zur Datenverarbeitung. Nach Art. 8 Abs. 1 JIRL ist eine Datenverarbeitung nur dann rechtmäßig, wenn sie zur Erfüllung einer Aufgabe der zuständigen Behörde erforderlich ist und auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedsstaaten erfolgt. Die Vorschrift muss nach Art. 8 Abs. 2 JIRL zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angeben.[16]

Dass die Einwilligung als Verarbeitungsgrund nicht vollständig ausgeschlossen ist, legen ErwGr 35 und 37 JIRL nahe. Dabei stellt ErwGr 35 zunächst die Situationen, in denen eine Einwilligung nicht erteilt werden kann, in den Vordergrund und erweckt den Eindruck, dass die Einwilligung als Grundlage der Verarbeitung in weiten Bereichen ausgeschlossen ist.[17] Nach ErwGr 35 S. 6 JIRL sollen die Mitgliedstaaten jedoch nicht daran gehindert sein, „durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung." Nach ErwGr 37 S. 5 JIRL kann eine Rechtsvorschrift die Verarbeitung besonderer Kategorien personenbezogener Daten erlauben, wenn die betroffene Person ausdrücklich zugestimmt hat.

aa) Ausdrückliche und spezifische Regelung

Daraus ist zu folgern, dass die Einwilligung im Anwendungsbereich der JIRL nur bei einer ausdrücklichen Regelung Rechtsgrundlage einer Datenverarbeitung sein kann. Es bedarf einer gesetzlichen Vorschrift, die die Polizei zu der Einholung einer Einwilligung ermächtigt. Sie kann Datenverarbeitungen, die gesetzlich nicht vorgesehen sind oder für die die gesetzlichen Voraussetzungen nicht vorliegen, nicht auf eine Einwilligung der betroffenen Person stützen.[18]

Zweitens deuten ErwGr 35 S. 6 und ErwGr 37 S.5 JIRL darauf hin, dass die Einwilligung im Anwendungsbereich der JIRL nur bezüglich spezifischer Fälle und Maßnahmen als Rechtsgrundlage der Datenverarbeitung geregelt werden kann, nicht aber als übergreifender Erlaubnistatbestand.[19] Der Gesetzgeber darf demnach nicht allgemein festlegen, dass eine Datenverarbeitung durch die Polizei zur Erfüllung ihrer Aufgaben zulässig ist, wenn die betroffene Person eingewilligt hat.

Zum Teil finden sich in den Polizei- und Landesdatenschutzgesetzen in Umsetzung der JIRL (bzw. Entwürfen hierzu) aber Regelungen, nach denen die Polizei umfangreich Daten auf Grundlage einer Einwilligung verarbeiten kann. So ist nach der neuen polizeilichen Generalklausel zur Datenerhebung in § 9 Abs. 1 Nr. 2 PolG NRW eine Datenerhebung nach Einwilligung der betroffenen Person grundsätzlich zulässig. Diese Vorschrift ist nicht spezifisch genug. Ähnlich unspezifisch ist Art. 28 Abs. 2 Nr. 2 BayDSG, der unter anderem Art. 6 Abs. 1 lit. a DSGVO im Geltungsbereich der JIRL für anwendbar erklärt und damit die Einwilligung zum allgemeinen Verarbeitungsgrund erhebt. Dies ist mit den beschriebenen Vorgaben der JIRL nicht vereinbar.

Allgemeine Vorschriften, die die Anforderungen an eine Einwilligung regeln, aber eine weitere Rechtsvorschrift für die Einwilligung erfordern, sind hingegen weniger problematisch – so etwa § 36 Abs. 1 BlnDSG, § 46 Abs. 1 HDSIG, § 33 Abs. 1 DSG RP, § 27 Abs. 1 LDSG SH, § 39 Abs. 1 ThürDSG sowie § 7 Sächsisches Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 (SächsDSUG). Diese Vorschriften sind andererseits nur eingeschränkt hilfreich, da sie lediglich einen allgemeinen Rahmen für die Voraussetzungen der Einwilligung regeln können.

bb) Inhaltliche Anforderungen

Die inhaltlichen Anforderungen an die Wirksamkeit einer Einwilligung müssen im Anwendungsbereich der JIRL mindestens so streng sein wie im Anwendungsbereich der DSGVO, da der Richtliniengeber gegenüber Einwilligungen wesentlich skeptischer war als der Verordnungsgeber.[20] Dass die Datenschutzgesetze für die Einwilligung im Anwendungsbereich der JIRL auf die Vorschriften der DSGVO (Art. 4 Nr. 11 und Art. 7 DSGVO) zurückgreifen,[21] ist vor diesem Hintergrund grundsätzlich sinnvoll.

Die Voraussetzung der Freiwilligkeit bedarf allerdings im Anwendungsbereich der JIRL einer weiteren Konkretisierung. Grenzen setzt der Freiwilligkeit zunächst ErwGr 35

16 Dabei ist unklar, worin der Unterschied zwischen „Ziel" und „Zweck" der Verarbeitung bestehen soll; vgl. *Bäcker*, in: Hill/Kugelmann/Martini, S. 63 (69). Beide Worte sind Synonyme (ebenso in der englischen Fassung „objective" und „purpose" und in der französischen „objektives" und „finalités"). Es ergibt sich auch nicht aus ErwGr 33 oder sonst im Zusammenhang mit der JIRL, dass zwischen Ziel und Zweck einer Verarbeitung zu unterscheiden wäre.

17 *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, § 1 Rn. 154.

18 *Bäcker/Hornung,* ZD 2012, 147 (150).

19 Ähnlich *Bäcker*, in: Hill/Kugelmann/Martini, S. 63 (71); vgl. ebenfalls spezifische Regelungen befürwortend *Johannes/Weinhold*, § 1 Rn. 157.

20 *Spiecker gen. Döhmann,* Stellungnahme zum Gesetzentwurf der Fraktionen der CDU und Bündnis 90/Die Grünen für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit – LT-Drs. 19/5728, S. 33; a.A.: BR-Drs. 110/17 (B), S. 43.

21 Dies erfolgt durch eine (abgeänderte) Übernahme des Wortlauts dieser Normen in den Umsetzungsvorschriften (§ 36 BlnDSG; § 46 HDISG; § 33 NDSG; § 38 DSG NRW; § 33 RPDSG; § 7 SächsDSUG; § 27 SHDSG; § 39 ThürDSG) oder dadurch, dass sie im Anwendungsbereich der JIRL für anwendbar erklärt werden (Art. 28 Abs. 2 Nr. 1 und 2 BayDSG; § 2 Abs. 6 BbgDSG; § 3 DSG-MV).

S. 3 und 4 JIRL. Demnach soll die Einwilligung „keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen", wenn „die zuständigen Behörden natürliche Personen auffordern oder anweisen [können], ihren Anordnungen nachzukommen". Bei der Aufforderung, einer rechtlichen Verpflichtung nachzukommen, bestehe keine Wahlfreiheit und daher kein Spielraum für eine freiwillige Einwilligung (ErwGr 35 Satz 5 JIRL). Im Falle einer Duldungs- oder Mitwirkungspflicht bei der Datenverarbeitung ist eine Einwilligung damit kategorisch ausgeschlossen.[22]

Um im Einzelfall abzusichern, dass eine Einwilligung freiwillig erteilt wird, ist vor allem wichtig, dass die betroffene Person präzise und vollständig über die Freiwilligkeit der Einwilligung, die Folgen ihrer Verweigerung und die Möglichkeit eines Widerrufes belehrt wird. Dieses Erfordernis hängt mit der Voraussetzung der Informiertheit der Einwilligung zusammen. Vorschriften, die die Einwilligung der betroffenen Person als Rechtsgrundlage der Datenverarbeitung vorsehen, müssen danach sicherstellen, dass die betroffene Person darüber informiert wird, dass sie frei über die Erteilung der Einwilligung entscheiden und diese jederzeit widerrufen kann sowie dass ihr keine Nachteile daraus entstehen, wenn sie die Einwilligung verweigert oder widerruft.

Die in den Gesetzen zur Umsetzung der JIRL vorgesehenen Pflichten genügen dem teilweise nicht. So ist beispielsweise in § 7 Abs. 4 S. 3 SächsDSUG vorgesehen, dass die Aufklärung über die Folgen einer Verweigerung der Einwilligung nur ausnahmsweise zu erfolgen hat. Dies ist unzureichend, da nicht davon auszugehen ist, dass die betroffene Person ihre Einwilligung regelmäßig in der Vorstellung erteilt, ihr stehe eine Wahlmöglichkeit gegenüber der Polizei zu. § 36 Abs. 4 S. 4 BlnDSG hingegen sieht den Hinweis auf die Folgen der Verweigerung einer Einwilligung grundsätzlich vor.

Auch sonst muss die betroffene Person über die für ihre Einwilligung bedeutenden Umstände informiert sein und die Auswirkungen ihrer Einwilligung zum Zeitpunkt der Abgabe erfassen können. So muss sie vor der Einwilligung in eine Datenverarbeitung mindestens wissen, welche ihrer Daten von wem zu welchem Zweck wie verarbeitet werden sollen.[23] Darüber hinaus muss der betroffenen Person ausreichend Zeit eingeräumt werden, um sich die Entscheidung zu überlegen und ggf. Rechtsrat einzuholen.[24] Dies kann nötig sein, da die betroffene Person häufig nicht einschätzen können wird, ob rechtliche Ausführungen der Behörde zu den Voraussetzungen der Datenerhebungsmaßnahme richtig sind. Im Anwendungsbereich der JIRL ist es stets im Sinne der entsprechenden Vorschriften der Umsetzungsgesetze notwendig, die betroffene Person über die Folgen der Verweigerung der Einwilligung zu belehren und sie zu informieren, ob die Maßnahme auch zwangsweise angeordnet werden kann.[25] So wird verhindert, dass diese eine Einwilligung erteilt, weil sie davon ausgeht, dass ihr ansonsten Sanktionen drohen oder sie zur Duldung der Maßnahme verpflichtet wird, obwohl dafür keine Rechtsgrundlage besteht bzw. die Voraussetzungen der Rechtsgrundlage nicht erfüllt sind.

2. Ausnahmen zu den Betroffenenrechten

Weitere Probleme bestehen im Zusammenhang mit der Umsetzung der Betroffenenrechte. Die JIRL enthält – ähnlich wie die DSGVO – weitreichende Rechte, über Datenverarbeitungsvorgänge informiert zu werden sowie auf diese einwirken zu dürfen.[26] Bei der Umsetzung der Regelungen im polizeilichen Bereich begegnen vor allem die im Zusammenhang mit den Betroffenenrechten vorgesehenen Ausnahmen Bedenken.

a) Ausnahmen zu Sicherheitszwecken

Die JIRL erlaubt die Regelung von Ausnahmen von Betroffenenrechten unter anderem, wenn die Einschränkung dieser Rechte zur Gewährleistung unbehinderter behördlicher Ermittlungen sowie Verfahren oder zum Schutz der öffentlichen oder nationalen Sicherheit notwendig ist.[27] Teilweise erscheinen die in den Gesetzen zur Umsetzung der JIRL zu diesen Zwecken vorgesehenen Ausnahmen allerdings zweifelhaft. Dies gilt etwa für Regelungen, die die Wahrung von Betroffenenrechten bei der Übermittlung von Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst pauschal von einer Zustimmung dieser Stellen abhängig machen. So stehen in § 12 Abs. 3 SächsDSUG die Benachrichtigungspflicht und in § 13 Abs. 3 SächsDSUG das Auskunftsrecht unter entsprechenden Vorbehalten. Zwar können in vielen Fällen der Übermittlung an die genannten Stellen Sicherheitsbelange die Beschränkung der Betroffenenrechte rechtfertigen. Dies aber ohne weitere Prüfung grundsätzlich anzunehmen und die Wahrung der Betroffenenrechte in entsprechenden Fällen von der Regel zur Ausnahme zu machen, erscheint aber als zu weitgehend.

Eine Prüfung, ob Sicherheitsbelange der Wahrung der Betroffenenrechte entgegenstehen, ist auch bei Übermittlung von Informationen an Nachrichtendienste nicht entbehr-

22 *Schwichtenberg*, DuD 2016, 605 (606).
23 *Gierschmann,* in: Gierschmann/Schlender/Stentzel/Veil, DSGVO, 2018, Art. 7 Rn. 77 ff.
24 *Schwichtenberg,* DuD 2016, 605 (607).
25 *Schwichtenberg,* in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. (2018), § 51 BDSG Rn. 6; *Stief,* StV 2017, 470 (476).
26 Im Unterschied zur DSGVO enthält die JIRL aber kein Widerspruchsrecht (Art. 21 DSGVO) sowie kein Recht auf Datenübertragbarkeit (Art. 20 DSGVO). Letzteres würde im polizeilichen Bereich auch kaum Sinn ergeben, da Betroffene etwa wenig Interesse daran haben dürften, über sie gespeicherte Informationen aus einer Polizeidatenbank in eine andere Datenbank zur Strafverfolgung übertragen zu lassen.
27 Vgl. Art. 13 Abs. 3 (Benachrichtigungspflicht), Art. 15 Abs. 1 (Auskunftsrecht) und Art. 16 Abs. 4 JIRL (Recht auf Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung).

lich. Dies gebietet die fundamentale Bedeutung der Betroffenenrechte für das Datenschutzrecht.[28] Auch die Datenschutzaufsichtsbehörden dürften im Übrigen regelmäßig in der Lage sein, eine Abwägung zwischen den Belangen des Datenschutzes und der öffentlichen Sicherheit vorzunehmen, so dass die Prüfung dieser Voraussetzung nicht ausschließlich auf die Nachrichtendienste verlagert werden sollte.

b) Bevormundende Ausnahmen

Während die zuvor betrachteten Ausnahmen zu Betroffenenrechten zumindest in ihrer Grundausrichtung noch nachvollziehbar sind, sehen die Gesetze zur Umsetzung der JIRL teilweise auch Ausnahmen vor, deren Zielrichtung schon überaus zweifelhaft ist. So enthalten einzelne Regelungen Ausnahmen von den Betroffenenrechten, die zumindest ihrem Wortlaut nach dazu dienen sollen, die Interessen der betroffenen Person, die selbst ein Recht geltend macht, zu schützen. So sieht eine Ausnahme von dem Recht auf Löschung in § 14 Abs. 2 S. 2 SächsDSUG vor, von einer verlangten Löschung abzusehen, „wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden".

Diese Regelung ist nicht von der JIRL gedeckt. Art. 16 Abs. 3 JIRL beschränkt die Möglichkeit, eine Einschränkung der Verarbeitung statt einer Löschung vorzusehen, im Wesentlichen auf die Fälle, dass die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann (Art. 16 Abs. 3 lit. a JIRL) sowie dass die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden müssen (Art. 16 Abs. 3 lit. b JIRL). Hier findet sich die in § 14 Abs. 2 S. 2 SächsDSUG vorgesehene Ausnahme nicht wieder.

Wie sich aus ErwGr 47 S. 4 JIRL[29] ergibt, sollen zusätzlich berechtigte Interessen betroffener Personen Ausnahmen von den Löschungspflichten ermöglichen. Dies findet in Art. 16 JIRL zwar nicht direkt Ausdruck, lässt sich aber aus Art. 4 und Art. 8 JIRL als Legitimierung der weiteren Verarbeitung herleiten. Verstünde man § 14 Abs. 2 S. 2 SächsDSUG so, dass dieser die Interessen eines dritten Betroffenen schützten soll, der die Löschung nicht verlangt hat, könnte dieser noch von der JIRL gedeckt sein. Datensätze können unterschiedliche Personen betreffen, von denen manche ein Interesse an einer Löschung haben, während dies bei anderen nicht der Fall ist.[30]

Allerdings bezeichnet der Wortlaut der Regelung allem Anschein nach mit „der betroffenen Person", deren Interessen der Löschung entgegenstehen können, die Person, die selbst die Löschung verlangt. Diese Person hat durch ihr Löschungsbegehren aber gerade zum Ausdruck gebracht, dass die Löschung in ihrem Interesse ist. Der Löschung entgegenzuhalten, die Person würde sich damit selbst schaden, erscheint als unzulässige Bevormundung, die dem Sinn und Zweck des Betroffenenrechts zuwiderläuft. Auch wenn § 14 Abs. 2 S. 2 SächsDSUG irrtümlich falsch formuliert sein sollte, erscheint die Regelung nicht mit Art. 16 Abs. 3 JIRL vereinbar. Noch mit der JIRL vereinbar erschiene die Regelung, würde sie unbestimmt auf die Interessen einer betroffenen Person[31] oder ausdrücklich auf die Interessen einer anderen Person abstellen.

c) Unverhältnismäßiger Aufwand

Zum Teil sehen die Gesetze zur Umsetzung der JIRL im polizeilichen Bereich noch weitere Ausnahmen von den Betroffenenrechten vor, deren Vereinbarkeit mit den Vorgaben der Richtlinie zumindest zweifelhaft ist. Ein „Klassiker" sind hierbei Regelungen, die aufgrund eines unverhältnismäßigen Aufwandes bei der Wahrung von Betroffenenrechten Ausnahmen von diesen vorsehen.[32]

So soll etwa nach § 44 Abs. 3 S. 1 Nr. 3 BlnDSG, § 32 Abs. 3 S. 1 PolG NRW in Verbindung mit § 50 Abs. 3 S. 1 Nr. 3 DSG NRW, § 53 Abs. 3 S. 1 Nr. 3 HDSIG sowie § 34 Abs. 3 Satz 3 LDSG Schleswig-Holstein ein unverhältnismäßiger Aufwand eine Ausnahme von dem grundsätzlichen Recht auf Löschung personenbezogener Daten begründen. Diesen Fall nennt Art. 16 Abs. 3 JIRL allerdings nicht als mögliche Ausnahme.[33] Die Regelung ist so zu verstehen, dass ein ökonomischer oder administrativer Aufwand nicht vorgebracht werden kann, um das Löschungsrecht einzuschränken.[34] Die genannten Regelungen sind damit mit der JIRL unvereinbar.

3. Befugnisse der Datenschutzaufsicht

Schließlich enthalten mehrere Landesregelungen zur Umsetzung der JIRL keine ausreichenden Befugnisse für die Datenschutzaufsicht.

a) Vorgaben der JIRL

Grundlage für die Befugnisse der Datenschutzaufsicht ist im Anwendungsbereich der JIRL deren Art. 47. Nach Abs. 1 S. 1 der Vorschrift haben die Mitgliedstaaten vorzusehen, dass jede Aufsichtsbehörde über wirksame Untersuchungsbefugnisse verfügt. Nach Art. 47 Abs. 2 JIRL sind zusätzlich wirksame Abhilfebefugnisse vorzusehen.

---

28 Vgl. zum Recht auf Auskunft Art. 8 Abs. 2 S. 2 GRCh.

29 „Insbesondere sollte statt der Löschung personenbezogener Daten die Verarbeitung eingeschränkt werden, wenn in einem konkreten Fall berechtigter Grund zu der Annahme besteht, dass eine Löschung die berechtigten Interessen der betroffenen Person beeinträchtigen könnte."

30 Vgl. BVerfGE 109, 279 (365).

31 So etwa §§ 43 Abs. 3 i.V.m. 35 Abs. 3 Nr. 1 ThürDSG, § 44 Abs. 3 S. 1 Nr. 1 BlnDSG, § 34 Abs. 3 S. 1 Nr. 1 LDSG SH, § 46 Abs. 3 S. 1 Nr. 1 LDSG RP, § 53 Abs. 3 S. 1 Nr. 1 HDSIG.

32 Vgl. hierzu die ebenfalls hinsichtlich ihrer Vereinbarkeit mit der JIRL problematischen §§ 57 Abs. 2, 58 Abs. 3 S. 1 Nr. 3, 66 Abs. 3 Nr. 3 BDSG.

33 Vgl. ähnlich zu den Ausnahmetatbeständen in Art. 15 Abs. 1 JIRL *Bäcker*, in: Hill/Kugelmann/Martini, S. 63 (82).

34 Vgl. *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 1244; *Schwichtenberg*, in: Kühling/Buchner, BDSG, § 58 Rn. 7.

Dazu können nicht nur Befugnisse zur (Ver-)Warnung gehören (Art. 47 Abs. 2 lit. a JIRL), sondern auch weitgehende Anweisungsrechte einschließlich des Rechtes, Verarbeitungsvorgänge einzuschränken oder zu verbieten (Art. 47 Abs. 2 lit. b und c JIRL).

Art. 47 JIRL erfordert zwar nicht, die in Abs. 2 der Vorschrift genannten Rechte wortlautgetreu umzusetzen. Das Gebot der Wirksamkeit dürfte aber zumindest minimale Befugnisse zu einer verbindlichen Einwirkung auf Datenverarbeitungen erfordern, die es ermöglichen, die unionsrechtlichen Vorgaben des Datenschutzrechtes zu schützen und eine gewisse Präventionswirkung gegenüber den Datenverarbeitern zu entfalten. Insofern lassen sich Parallelen zu dem Gebot der Wirksamkeit von Sanktionen zur Ahndung von Verstößen gegen unionsrechtliche Verhaltensnormen ziehen.[35] Eine funktionsfähige und mit ausreichenden Befugnissen ausgestattete Datenschutzaufsicht ist essentiell, um die Einhaltung und Durchsetzung des Datenschutzrechts zu gewährleisten. Dies ist auch dem Umstand geschuldet, dass die Betroffenen selbst oftmals nicht über die Mittel verfügen oder ausreichende Anreize haben, um Datenschutzverstöße selbst zu verfolgen.

Für die Notwendigkeit, konkrete Rechte der Aufsichtsbehörden zur Einwirkung auf Datenverarbeitungsvorgänge vorzusehen, spricht auch Art. 46 Abs. 1 lit. a JIRL, wonach jeder Mitgliedstaat vorsieht, „dass jede Aufsichtsbehörde in seinem Hoheitsgebiet die Anwendung der nach dieser Richtlinie erlassenen Vorschriften sowie deren Durchführungsvorschriften überwacht und durchsetzt". Eine Durchsetzung im engeren Sinne ist ohne verbindliche Einwirkungsbefugnisse nicht vorstellbar.

Im Ergebnis müssen die Aufsichtsbehörden nach Art. 47 Abs. 2 JIRL damit zumindest das Recht haben, konkrete Weisungen bezüglich einzelner Datenverarbeitungsvorgänge zu erteilen.[36] Auch die Art. 29-Datenschutzgruppe hat sich auf den Standpunkt gestellt, dass wirksame Abhilfebefugnisse im Sinne von Art. 47 Abs. 2 JIRL „verbindliche Befugnisse der Datenschutzaufsichtsbehörden, um bestimmte korrigierende Maßnahmen anzumahnen, zu verhängen oder anzuordnen und verbindliche Entscheidungen gegenüber Verantwortlichen zu erlassen"[37] erfordern.

Da auch in der polizeilichen Arbeit Potentiale zum Missbrauch personenbezogener Daten bestehen und entsprechende Fälle – etwa im Zusammenhang mit polizeilichen Datenbanken – bekannt sind, erschiene es naheliegend, die Datenschutzaufsicht in diesem Bereich mit ähnlichen Befugnissen auszustatten wie im Anwendungsbereich der DSGVO (nach deren Art. 58). Dies ist allerdings nicht durch alle Umsetzungen der JIRL geschehen.

b) Abgeschwächte Befugnisse in Rheinland-Pfalz

So sind etwa in der Umsetzung der JIRL in Rheinland-Pfalz nur abgeschwächte Befugnisse der Datenschutzbeauftragten vorgesehen. Die Befugnis des LfDI Rheinland-Pfalz, nach § 42 Abs. 2 LDSG RP Anordnungen zur Beseitigung von Datenschutzverstößen zu treffen, ist auf Fälle beschränkt, in denen „dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist."

Dies genügt einer wirksamen Abhilfebefugnis nicht. Das Erfordernis eines erheblichen Verstoßes schränkt die Handlungsmöglichkeiten der Datenschutzaufsicht zu stark ein. Es ist unklar, ab welcher Schwelle ein erheblicher Verstoß vorliegen soll. Mit dem Kriterium der „schwerwiegenden Persönlichkeitsbeeinträchtigung" fand sich in einzelnen Regelungen des BDSG a.F.[38] ein ähnlich unklarer Begriff, zu dem sich spezifisch in Bezug auf das Datenschutzrecht keine klare Handhabe in Literatur und Rechtsprechung herausbildete.[39] Die Erheblichkeit eines Verstoßes festzustellen wird auch bei klaren Datenschutzverstößen eine zusätzliche Einzelfallbetrachtung erfordern, die eine wirksame Tätigkeit der Datenschutzaufsicht erschweren dürfte. Dass nicht erhebliche Verstöße gewissermaßen als „Kavaliersdelikte" hingenommen werden müssen, ohne dass für die Aufsicht eine Abhilfemöglichkeit besteht, genügt der Voraussetzung der Wirksamkeit im Sinne von Art. 47 Abs. 2 JIRL nicht.

c) „Zahnlose" Regelungen in Hessen, Thüringen und Berlin

Sogar noch weiter eingeschränkt sind die Befugnisse der Aufsicht im Anwendungsbereich der JIRL in den Regelungen von Hessen,[40] Thüringen[41] und Berlin[42].[43] Nach § 7 Abs. 6 Satz 1 ThürDSAnpUG-EU hat der LfDI Thüringen bei Verstößen gegen das Datenschutzrecht außerhalb des Anwendungsbereiches der DSGVO zunächst eine Beanstandung auszusprechen und eine Stellungnahme von dem Verantwortlichen einzuholen. Nach Satz 5 der Vorschrift kann er erst weitere Maßnahmen von der obersten Landesbehörde und der Aufsichtsbehörde einfordern (aber nicht selbst treffen), wenn der Verstoß auf die Beanstandung nicht behoben wird. Eine ähnliche Regelung findet sich in § 13 Abs. 2 BlnDSG. Auch hiernach ist die Berliner LfDI im Anwendungsbereich der JIRL im Grunde auf das Instrument der Beanstandung beschränkt. So werden der Datenschutzaufsicht im polizeilichen Bereich die Zähne gezogen. Die Beanstandung selbst hat noch keine Sanktionswirkung und führt lediglich dazu,

35 Vgl. hierzu *Golla*, in: Auernhammer, DSGVO/BDSG, 6. Aufl. (2018), Art. 84 DSGVO Rn. 4 f. m.w.N.

36 Zurückhaltender, aber im Ergebnis ebenfalls Einwirkungsbefugnisse befürwortend *Bäcker*, in: Hill/Kugelmann/Martini, S. 63 (83 f.).

37 Art.-29-Datenschutzgruppe, Stellungnahme zu einigen grundlegenden Fragestellungen der Richtlinie Justiz/Inneres, EU 2016/680, WP 258, angenommen am 29. November 2017, S.30.

38 §§ 42a Satz 1, 14 Abs. 2 Nr. 8, 38 Abs. 5 S. 2.

39 *Golla*, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, 2015, S. 208 f.

40 § 14 Abs. 3 HDSIG.

41 § 7 Abs. 6 ThürDSAnpUG-EU.

42 § 13 Abs. 2 BlnDSG.

43 In dem Entwurf des LDSG Schleswig-Holstein bestand zunächst ein ähnliches Problem, das aber durch Einfügung des § 64 Abs. 4 LDSG Schleswig-Holstein behoben wurde; vgl. LfDI Hamburg, Schriftliche Anhörung des Innen- und Rechtsausschusses des schleswig-holsteinischen Landtags zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, S. 6 ff.

dass der Adressat dazu verpflichtet wird, sich mit ihrem Gegenstand zu befassen. Eine echte Einwirkungmöglichkeit hat der Datenschutzbeauftragte damit nicht. Es fehlt an wirksamen Abhilfebefugnissen im Sinne von Art. 47 Abs. 2 JIRL und damit an einer ausreichenden Umsetzung der Vorschrift.[44]

IV. Fazit: Bedarf zur Nachbesserung

Die bisherigen Erfahrungen mit der Umsetzung der JIRL im polizeilichen Bereich zeigen einige strukturelle Regelungsfehler auf diesem Gebiet. Diese betreffen unter anderem zentrale Themen wie die Tauglichkeit der Einwilligung als Grundlage von Datenverarbeitungen im polizeilichen Bereich und die Aufsichtsbefugnisse der Landesdatenschutzbeauftragten. Diese Aspekte haben mehrere Landesgesetzgeber fehlerhaft umgesetzt bzw. sind dabei, dies zu tun. Auch angesichts der Risiken und Missbrauchspotentiale, die mit den immensen polizeilichen Datenbeständen verbunden sind, verdient dieser Regelungsbereich eine größere Aufmerksamkeit und sorgfältigere Regelungen. Der polizeiliche Datenschutz darf im Schatten von DSGVO und anderweitigen Polizeirechtsreformen nicht vernachlässigt werden. Es ist zu hoffen, dass in den noch laufenden Gesetzgebungsverfahren sowie in Ergänzung der abgeschlossenen Verfahren Nachbesserungen zumindest in den zentralen Bereichen erfolgen.

[44] So auch Thüringer LfDI, Stellungnahme zum Gesetzentwurf Thüringer Datenschutz-Anpassungs- und Umsetzungsgesetz EU, S. 23 f.