NETZWERK DATENSCHUTZEXPERTISE

Die EU-Richtlinie für den Datenschutz bei Polizei und Justiz

Stand: 1.02.2016

Inhalt

Dr. Thilo Weichert
Waisenhofstr. 41, 24103 Kiel
0431 9719742
weichert@netzwerk-datenschutzexpertise
www.netzwerk-datenschutzexpertise.de

1 Einleitung

Als am 15.12.2015 die Trilog-Verhandlungen über die grundlegende Reform des europäischen Datenschutzrechts abgeschlossen waren, berichteten die Medien umfassend über die Europäische Datenschutzgrundverordnung (EU-DSGVO), also das künftig gültige allgemeine Datenschutzrecht in der Europäischen Union (EU). Praktisch keine Beachtung fand der kleine Bruder dieser Regelung, über den sich Parlament, Rat und Kommission der EU zeitgleich einigten: die EU-Richtlinie für den Datenschutz bei Polizei und Justiz – genauer die „Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“. Das Dokument war und ist im Netz von der EU derart versteckt abgelegt, dass der grüne Europaabgeordnete Jan-Phillipp Albrecht dieses leichter zugänglich veröffentlichen musste:

> https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPD_consolidated_LIBE-vote-2015-12-17.pdf

Natürlich hat die EU-Richtlinie für Polizei und Justiz (im Folgenden zitiert als „Richtlinie“) nicht die gleiche Relevanz wie die EU-DSGVO, doch ist sie ein Meilenstein für den europäischen Datenschutz in diesem Sektor. Der Datenschutz in den hochsensiblen und eingriffsintensiven Bereichen Strafverfolgung und Gefahrenabwehr wird sich künftig europaweit hieran orientieren. Die Mitgliedstaaten werden in dieser Richtlinie zur Gesetzgebung über die polizeiliche und strafverfolgende Datenverarbeitung verpflichtet. In Deutschland betrifft dies nicht nur den Bund, sondern insbesondere auch die für das allgemeine Polizeirecht zuständigen Bundesländer. Es gibt also genug Gründe, sich die Richtlinie genau anzusehen.

2 Geschichte

Der Vorschlag der EU-Kommission vom 25.01.2012 für eine grundlegende Reform des europäischen Datenschutzrechts umfasste neben dem Entwurf einer EU-DSGVO auch den einer Richtlinie für Polizei und Justiz, mit welcher der Rahmenbeschluss der EU-Kommission 2008/977/JI[1] ersetzt werden soll[2]. Die Datenverarbeitung durch Polizei und Justiz gehörte früher der „dritten Säule“ der EU an, die bei weitem nicht so stark reguliert war wie die übrige staatliche Verwaltung und die Wirtschaft. Der bis heute gültige Rahmenbeschluss beschränkt sich ausschließlich auf den grenzüberschreitenden Datenverkehr und machte keinerlei Aussagen über die interne Organisation der Datenverbreitung bei Polizei und Justiz. Dies lässt sich nicht mehr aufrecht halten. Mit den Verträgen von Lissabon wurde dieser Bereich „vergemeinschaftet“. In diesem Zusammenhang wurde Ende 2009 auch die Europäische Grundrechtecharta (EUGRCh) in Kraft gesetzt, die in den Art. 7, 8 und 47 Privatsphäre, Telekommunikationsgeheimnis, Datenschutz und einen effektiven Rechtsschutz zusichern. Diese Garantien gelten auch für die Bereiche der Strafverfolgung und der Gefahrenabwehr.

[1] ABl. L 350 v. 30.12.2008, S. 60
[2] 2012/0010 (COD)

Im sog. Stockholmer Programm[3] hatte der Rat der EU die Kommission ersucht, die bestehenden Rechtsinstrumente zum Datenschutz zu bewerten und im Bedarfsfall Initiativen vorzulegen. Die EU-Kommission erstellte einen Aktionsplan zur Umsetzung des Stockholmer Programms[4], in dem zwecks „konsequenter Anwendung des Grundrechts auf Datenschutz“ eine Stärkung der „Position der EU bezüglich des Schutzes personenbezogener Daten bei allen EU-Maßnahmen, einschließlich jener in den Bereichen Strafverfolgung und Kriminalprävention sowie in unseren internationalen Beziehungen“ vorgesehen ist.

In Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ist der Grundsatz verankert, dass jede Person das Recht auf Schutz ihrer personenbezogenen Daten hat. Art. 16 Abs. 2 AEUV schafft eine besondere Rechtsgrundlage für den Erlass von Datenschutzvorschriften, die auch für die polizeiliche und justizielle Zusammenarbeit in Strafsachen gilt. Vom 04.11.2010 bis 15.01.2011 erfolgte eine Konsultation zum Gesamtkonzept der Kommission für den Datenschutz in der EU. Mit Entschließung vom 06.07.2011 nahm das EU-Parlament einen Bericht an, der das Kommissionskonzept für die Reform des Datenschutzes unterstützt.

Ähnlich wie bei der EU-DSGVO stand auch bei der geplanten Regulierung im Bereich Polizei/Justiz das in Art. 5 Abs. 3 EU-Vertrag (EUV) niedergelegte Subsidiaritätsprinzip zur Diskussion, wonach die EU nur tätig werden darf, sofern und soweit die angestrebten Ziele von den Mitgliedstaaten allein nicht ausreichend verwirklicht werden können und wegen ihres Umfangs und ihrer Wirkung auf Unionsebene besser zu verwirklichen sind. Der Deutsche Bundesrat erhob Subsidiaritätsrügen gegen die EU-DSGVO und die Richtlinie. Beides wurde von der EU zurückgewiesen. Da der Bedarf der Strafverfolgungsbehörden an einem schnellen Datenaustausch zur Verhütung und Bekämpfung von Kriminalität ein unionsweites einheitliches Datenschutzniveau erfordert, sei eine Regulierung nötig. Eine Richtlinie wurde als einzig verhältnismäßig angesehen, um den Mitgliedstaaten bei der Umsetzung der Grundsätze und der Vorschriften noch einen Spielraum zu belassen. Neben den schon erwähnten Grundrechten aus Art. 7, 8 und 47 EUGRCh ist das Diskriminierungsverbot im Hinblick auf Rasse, ethnische Herkunft, genetische Merkmale, Religion, Weltanschauung, politische oder sonstige Anschauung, Behinderung und sexuelle Ausrichtung (Art. 21 EUGRCh) von Relevanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder gab am 11.06.2012 eine Stellungnahme zum Kommissionsentwurf ab. Die Artikel-29-Arbeitsgruppe erstellte auch eine Stellungnahme mit Datum vom 26.02.2013 mit den vier Schwerpunkten: Verarbeitung von Daten nichtverdächtiger Personen, Betroffenenrechte, Datenschutzfolgenabschätzung und Befugnisse der Datenschutzaufsicht.

Der Vorschlag der EU-Kommission wurde intensiv vom EU-Parlament behandelt und am 12.03.2014 mit Änderungsvorschlägen mit großer Mehrheit angenommen. Berichterstatter war der griechische Abgeordnete Dimitros Droutsas. Die daraufhin erfolgende Behandlung im EU-Rat wurde am 09.10.2015 abgeschlossen.

3 Inhalt der Richtlinie

Zum Zeitpunkt des Verfassens dieses Artikels lag noch keine deutschsprachige Version der Richtlinie vor und auch noch kein Beschlusstext mit der endgültigen Durchnummerierung der Artikel und der

[3] ABl. C 115 v. 04.05.2010, S. 1
[4] Com(2010) 171 endg.

erläuternden Erwägungsgründe (EG). Die Gliederung der Richtlinie kann der Aufstellung am Ende dieses Beitrags entnommen werden. Dabei wird die Zählweise der Artikel sowohl im Rahmen der Entwurfsbehandlung wie auch in der voraussichtlichen Beschlussfassung dargestellt. Bei der folgenden Darstellung wird die erwartete künftige Artikel-Zählung zu Grunde gelegt.

Die Richtlinie gibt nur einen Regelungsrahmen vor, bei dem den EU-Mitgliedstaaten weitgehende Spielräume gelassen werden. Es wird definitiv klargestellt, dass die nationalen Regelungen ein höheres Schutzniveau als von der Richtlinie vorgegeben gewähren dürfen (Art. 1 Abs. 2). Die Vagheit vieler Regelungen führt dazu, dass es den Mitgliedstaaten oft erlaubt wird, nationale Ausnahmen von Schutzvorschriften vorzusehen.

3.1 Anwendungsbereich

In Art. 1 wird der Gegenstand der Regelung dargestellt: Es geht um den ungehinderten Austausch personenbezogener Daten zwischen Behörden der Polizei und der Justiz innerhalb der EU und den Grundrechtsschutz der davon betroffenen Personen, insbesondere den Datenschutz. Erfasst werden nur Verarbeitungen, die folgende Zwecke verfolgen: „Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder die Durchführung von Kriminalstrafen, einschließlich der Schutz vor und die Verhütung von Gefahren für die öffentliche Sicherheit“ (Art. 1 Abs. 1). Werden von privaten oder öffentlichen Stellen andere Zwecke verfolgt, so ist die EU-DSGVO anzuwenden (Art. 9 Abs. 2). Was unter öffentlicher Sicherheit verstanden wird, ist nicht eindeutig definiert. Erfasst sein sollen auch Zwangsmaßnahmen der Polizei bei Demonstrationen, Sportereignissen und Unruhen[5]. Keine Anwendung findet die Richtlinie für EU-Institutionen sowie für Vorgänge, die nicht unter EU-Recht fallen (Art. 2 Abs. 3). Nicht erfasst sein sollen zudem Maßnahmen für die nationale Sicherheit[6]. Dies bedeutet, dass neben dem Verteidigungsbereich in Deutschland wohl auch die Inlands- und Auslandsgeheimdienste (Verfassungsschutz, MAD, BND) ausgenommen sein sollen. Die Richtlinie ist nicht auf Eurojust und Europol anwendbar. Sie erwähnt diese Einrichtungen nicht einmal in den Erwägungsgründen. Es wäre wünschenswert, wenn insofern zumindest mittelfristig einheitliche Standards eingeführt würden.

Schon aus der gemeinsamen Behandlung von EU-DSGVO und der Richtlinie zeigt sich, dass beide Rechtsmaterien eng aufeinander abgestimmt sind und sich gegenseitig ergänzen sollen. Dies führt zu Parallelen bei den Begriffsbestimmungen (Art. 3), bei der Verantwortlichkeit (Art. 19 ff.), bei den internen Datenschutzbeauftragten (Art. 32-34) oder bei den Aufsichtsbehörden (Art. 41 ff.). Die Richtlinie ist nicht nur bei Polizei und Staatsanwaltschaften anwendbar, sondern auch auf Gerichte, außer wenn diese in ihrer unabhängigen gerichtlichen Funktion tätig sind. National darf geregelt werden, dass selbst unabhängige Strafverfolgungsbehörden ausgenommen werden können[7]. Dies gilt aber nicht für Deutschland, da hier, entgegen mancher staatsanwaltlichen Behauptung, keine solche quasi-richterliche Unabhängigkeit besteht. Erfasst wird nicht nur die automatisierte, sondern auch die Datenverarbeitung in analogen Dateien (Art. 2 Abs. 2).

3.2 Zulässigkeit der Datenverarbeitung

In Art. 4 Abs. 1 werden die Grundprinzipien der Datenverarbeitung bzw. des Datenschutzes dargestellt, u. a. die Zweckbindung, die Verhältnismäßigkeit („angemessen“, „nicht exzessiv“) und die

[5] EG 11a/12
[6] EG 11b/14
[7] EG 55/80

Erforderlichkeit. Die Zweckänderung wird unter einen nicht erkennbar eingeschränkten nationalen Gesetzesvorbehalt gestellt (Art. 4 Abs. 2).

Die Richtlinie enthält keine eigenständigen Erlaubnisnormen, sondern macht nur Vorgaben hierfür, die in den Mitgliedstaaten erlassen werden. Da in Deutschland insofern ein umfassendes Regelungsregime besteht, das in den wesentlichen Aspekten inhaltlich der Richtlinie entspricht, kann der bestehende Rahmen beibehalten werden. Die Richtlinie differenziert auch nicht danach, ob und wie Daten verdeckt erhoben werden. Hinsichtlich sensibler Daten werden eine strenge Erforderlichkeitsprüfung und zusätzliche Sicherungen gefordert (Art. 8, 9 Abs. 2 u. 3). Detailliertere Anforderungen an die nationalen Normen oder (Beweis-) Verwertungsverbote sind nicht vorgesehen. Ebenso fehlen, wie vorgeschlagen wurde, Aussagen über auf Einwilligung basierende Datenverarbeitungen.

Angesichts der Weite der vorgegebenen materiellen Regelungen wird es jetzt darauf ankommen, welche Grenzen der Europäische Gerichtshof (EuGH) angesichts Art 8 EUGRCh, der als Maßstab für die Auslegung der gesamten Richtlinie herangezogen werden kann, setzt (s. u. 5).

Anders als zunächst im Kommissionsvorschlag ist in Art. 5 vorgesehen, dass im nationalen Recht Lösch- und Prüffristen und entsprechende Verfahren geregelt werden müssen. Art. 6 sieht vor, dass hinsichtlich der Rollen der Betroffenen bei der Verarbeitung differenziert wird, und zwar ob diese erfasst sind als Verdächtige, Verurteilte, Opfer, Zeugen, Hinweisgeber. Eine weitere Differenzierung ist nach der sachlichen Richtigkeit und Zuverlässigkeit, also dem Grad der Wahrscheinlichkeit, vorgesehen. Erweist sich die Unrichtigkeit oder Unvollständigkeit, so müssen entsprechende Korrekturen und bei Übermittlungen Benachrichtigungen vorgenommen werden (Art. 7).

3.3 Betroffenenrechte

Zwar sind in Art. 13 umfassende Informationspflichten gegenüber den Betroffenen hinsichtlich verarbeitende Stelle, Zweck, Beschwerde- und Auskunftsrecht, evtl. Rechtsgrundlage, Speicherfrist, Empfänger und verdeckte Erhebung vorgesehen, doch können diese Ansprüche durch nationale Vorschriften wieder ausgehebelt werden, wenn dies in irgendeiner Weise die Aufgabenwahrnehmung oder die Rechte Dritter gefährdet. Besonders problematisch ist, dass es möglich sein soll, ganze Kategorien von Daten von der Informationspflicht auszunehmen (Art. 13 Abs. 4, s. u. 4.1). Entsprechend wird das in Art. 14 vorgesehene Auskunftsrecht in Art. 15 eingeschränkt. Im Verweigerungsfall ist darüber zu informieren, dass die Datenschutzaufsicht eingeschaltet werden kann (Art. 15 Abs. 3 S. 3). Die Datenschutzaufsicht kann auch dafür vorgesehen werden, die Betroffenenrechte wahrzunehmen (Art. 17).

3.4 Verantwortlichkeit

In den Art. 18 ff. sind Regelungen zur Verantwortlichkeit, zur gemeinsamen Verantwortlichkeit (Art. 21) und zur Auftragsdatenverarbeitung (Art. 22) enthalten. Diese entsprechen den bestehenden sowie den in der EU-DSGVO geplanten Regelungen. In Art 20 wird explizit „Data protection by Design and by Default“ geregelt. Pseudonymisierung und Datensparsamkeit werden erwähnt. Danach wird es verpflichtend, den Zugriff auf Daten zweckspezifisch und aufgabenbezogen zu begrenzen. Doch diese Vorgabe wird dadurch relativiert, dass als Konkretisierung nur klargestellt wird, dass Daten grds. nicht einer unbegrenzten Personengruppe bereitgestellt werden dürfen (Art. 20 Abs. 2 S. 2).

Alle Datenverarbeitungsprozesse sind gemäß Art. 24 zu dokumentieren bzgl. Verantwortlichkeit, Datenschutzbeauftragtem, Zweck, Empfängerkategorien, Profiling, Drittstaatenübermittlung,

Rechtsgrund, Auftragsdatenverarbeitungen, evtl. Löschfristen und technisch-organisatorischen Sicherungsmaßnahmen. Zudem ist in Art. 25 eine Protokollierungspflicht bei folgenden Vorgängen vorgesehen: Erhebung, Veränderung, Abfrage, Weitergabe, Kombination, Löschung; bei Abfragen und Weiterleitungen sind Zweck und Zeitpunkt und, soweit möglich, die handelnde Person aufzuzeichnen. Dokumentationen sind der Datenschutzaufsicht zur Verfügung zu stellen, Protokolle auf Anfrage. Es besteht eine generelle Pflicht zur Kooperation mit der Aufsicht (Art. 26)

Beim Einsatz neuer Technologien und im Hinblick auf besondere Grundrechtsgefahren ist ein „Data Protection Impact Assessment“, also eine Datenschutzfolgenabschätzung, vorgesehen (Art. 27). Ergibt sich hierbei ein hohes Risiko, so muss die Datenschutzaufsicht eingebunden werden. Innerhalb von 6 Wochen nach der Einbeziehung kann, soweit das nationale Recht dies vorsieht, die Aufsicht Warn- und Untersagungsfunktionen wahrnehmen (Art. 28 Abs. 5). Eine Pflicht zur Beteiligung besteht zudem bei der Vorbereitung von regulativen und gesetzgeberischen Maßnahmen (Art. 28 Abs. 2).

Anders als in der EU-DSGVO werden in Art. 29 die Datensicherheitsmaßnahmen als Katalog entsprechend der Anlage zu § 9 BDSG aufgeführt. Die modernen Datenschutz-Schutzziele werden nur ansatzweise oder überhaupt nicht erwähnt. In den Art. 30, 31 ist die unverzügliche „Meldung einer Verletzung“, also eine Breach Notification gegenüber der Datenschutzaufsicht und in speziellen engen Fällen gegenüber den Betroffenen vorgesehen. Die Art. 32 bis 34 enthalten verpflichtende Regelungen zur Ernennung, zur Stellung und zu den Aufgaben eines (internen) Datenschutzbeauftragten.

3.5 Datenübermittlung ins Drittausland

In den Art. 35-39 sind die materiellen Anforderungen an Datenübermittlungen in Drittländer geregelt. Grundsätzlich müssen folgende Voraussetzungen vorliegen: Erforderlichkeit, Zuständigkeit des Empfängers, Datenfreigabe durch Herkunftsland bei erhaltenen Daten und angemessenes Datenschutzniveau.

Fehlt es an einem zuvor festgestellten angemessenen Datenschutz beim Empfänger, kann dennoch eine Übermittlung erfolgen, wenn dies unter Berücksichtigung aller Umstände vom Ursprungsland zugelassen wird. Eine weitere Ausnahme von Erfordernis eines hinreichenden Datenschutzstandards besteht bei Erforderlichkeit für die Verhinderung einer unmittelbaren ernsthaften Gefahr für die öffentliche Sicherheit, wenn die Zustimmung des Ursprungslands nicht erlangt werden könnte. Dieses muss nachträglich informiert werden (Art. 35 Abs. 2, 3).

Nicht erwähnt wird, aber selbstverständlich sein sollte, dass Übermittlungen innerhalb der EU wie auch in Drittländer den nationalen Übermittlungsregelungen, wie sie auch zwischen Behörden im eigenen Land gelten, entsprechen müssen. Keine weitergehenden Einschränkungen bestehen, wenn die EU-Kommission festgestellt hat, dass im Empfängerland ein angemessenes Datenschutzniveau besteht. Bei der Kommissionsentscheidung sind folgende Aspekte relevant: rechtsstaatliches Verfahren, eine unabhängige Datenschutzkontrollinstanz und internationale Datenschutzverpflichtungen. Die Kommission muss laufend überprüfen, ob die Voraussetzungen weiterhin vorliegen. Ist dies nicht der Fall, ist die Angemessenheitsfeststellung zurückzunehmen bzw. zu ändern und es sind Verhandlungen mit dem Empfängerland aufzunehmen.

Fehlt es an einer allgemeinen Angemessenheitsfeststellung, so kann die Datenübermittlung mit spezifischen Sicherungen im Einzelfall legitimiert werden (Art. 37). Besteht insofern kein rechtlich bindendes Instrument, so muss die Datenschutzaufsicht informiert werden.

Schließlich dürfen Übermittlungen ohne jede Datenschutzsicherung erfolgen, wenn dies erforderlich ist für den Schutz eines lebenswichtigen Interesses des Betroffenen oder einer anderen Person, bei Vorliegen einer nationalen Regelung zum Schutz legitimer Betroffeneninteressen, zur Verhütung einer unmittelbaren ernsthaften Gefahr für die öffentliche Sicherheit entweder des Mitgliedstaats oder eines anderen Landes, in einzelnen Fällen für Zwecke nach Art. 1 Abs. 1 (Generalklausel) oder im Einzelfall zur Ausübung und Durchsetzung rechtlicher Interessen nach Art. 1 Abs. 1 (Art. 38 Abs. 1). Generell soll gelten, dass eine Übermittlung unzulässig ist, wenn die Behörde feststellt, dass die schutzwürdigen Betroffeneninteressen gegenüber dem öffentlichen Interesse an der Datenübermittlung überwiegen (Art. 38 Abs. 2). Beachtet werden soll, dass das übermittelte Daten nicht zur Begründung, Verwendung oder Umsetzung einer Todesstrafe oder einer anderen Form grausamer oder unmenschlicher Behandlung genutzt werden[8]. Die Übermittlung muss mit Zeitangabe, Empfänger und rechtfertigendem Grund dokumentiert werden.

Art. 39 sieht eine weitere Ausnahme im Einzelfall bei Übermittlungen an beliebige Dritte vor, wenn dies unbedingt notwendig ist für die Aufgabenerfüllung der übermittelnden Stelle und diese feststellt, dass Grundrechte gegenüber den öffentlichen Interessen an der Übermittlung nicht überwiegen, eine Übermittlung an die zuständige Stelle im Empfängerland keinen Erfolg verspricht, diese, soweit sinnvoll, informiert wird und dem Empfänger der spezifische Übermittlungszweck mitgeteilt wird. Dies kann in einem internationalen Abkommen vereinbart sein. Die Aufsichtsbehörde der übermittelnden Behörde muss informiert werden (Art. 39).

3.6 Datenschutzaufsicht

Die Art. 41 bis 49 regeln die unabhängige Datenschutzkontrolle. Diese ist an die Regelungen in der EU-DSGVO angelehnt. Sie muss unabhängig sein und mit personellen, technischen und finanziellen Ressourcen ausgestattet sein, um ihre Aufgaben und Befugnisse effektiv umsetzen zu können (Art. 42). Die in der EU-DSGVO vorgesehenen Behörden können auch als Aufsicht im Polizei- und Justizbereich eingesetzt werden.

Die Aufgaben der Datenschutzaufsicht liegen in der Datenschutzkontrolle gemäß Art. 46 der Richtlinie, der Öffentlichkeitsarbeit, der Beratung von Parlament und öffentlichen Stellen, der Fortbildung verantwortlicher Stellen, der Bearbeitung von Betroffenenanfragen und -beschwerden, der Rechtmäßigkeitskontrolle bei der Auskunftserteilung, der (europaweiten und internationalen) Zusammenarbeit mit anderen Aufsichtsbehörden (Art. 50), der Durchführung von Untersuchungen, der Beobachtung relevanter Entwicklungen, der Beratung bei der Datenschutzfolgenabschätzung und der Mitarbeit im Europäischen Datenschutzausschuss (Art. 51).

Die Datenschutzaufsicht hat umfassende Ermittlungsbefugnisse sowie „wirksame Einwirkungsbefugnisse“. Dazu zählen Beanstandungen, Anordnungen an die verantwortliche Stelle im Hinblick auf unzulässige Formen der Datenverarbeitung bis hin zu befristeten oder vollständigen Untersagungen bestimmter Verfahren (Abs. 47 Abs. 1, 2). Außerdem ist im nationalen Recht vorzusehen, dass die Aufsichtsbehörde die Befugnis erhält, Datenschutzverstöße einem justiziellen Verfahren zuzuführen (Art. 47 Abs. 5). Über wirksame Mechanismen muss gewährleistet werden, dass die zuständigen Aufsichtsbehörden vertraulich über Datenschutzverstöße unterrichtet werden können (Art. 48). Mit der Kooperationsbefugnis gegenüber anderen Aufsichtsbehörden korrespondiert eine grds. unentgeltliche Kooperationspflicht (Art. 50 Abs. 4-8). Dem Europäischen Datenschutzausschuss

[8] EG 49/71

kommen, anders als nach der EU-DSGVO, keine Entscheidungsbefugnisse zu. Die Aufgaben bestehen vielmehr in der Beratung, der Herausgabe von Richtlinien, der Prüfung, der Abgabe von Stellungnahmen, der Förderung von Kooperation, Schulung und Forschung.

3.7 Rechtsschutz und Umsetzung

Gemäß Art. 52 hat jeder Betroffene das Recht, sich mit einer Beschwerde wegen eines möglichen Datenschutzverstoßes an eine Aufsichtsbehörde zu wenden. Ist diese nicht zuständig, so leitet diese die Beschwerde an die zuständige Stelle weiter. Die Aufsichtsbehörde informiert den Betroffenen über den Fortschritt und das Ergebnis der Beschwerde einschließlich der Möglichkeiten für gerichtlichen Rechtsschutz. Gegen Entscheidungen der Aufsichtsbehörde sowie wegen deren Untätigkeit kann gerichtlicher Rechtsschutz erlangt werden (Art. 53). Ein gerichtlicher Rechtsbehelf ist auch gegen die für die Verarbeitung verantwortliche Stelle oder den Auftragsdatenverarbeiter gegeben (Art. 54). Im nationalen Recht ist auch vorzusehen, dass Einrichtungen, Organisationen oder Verbände das Recht haben, im Namen des oder der Betroffenen die Beschwerde- und Klagerechte nach den Art. 52, 53 und 54 wahrzunehmen.

Im nationalen Recht sind zudem Haftungs- und Sanktionsregelungen vorzusehen (Art. 56, 57).

Zur Umsetzung der Richtlinie gibt es ein Ausschussverfahren im Sinne der Verordnung (EU) Nr. 182/2011 (Art. 58). Der Rahmenbeschluss 2008/977/JHA wird aufgehoben (Art. 59). Internationale Abkommen, die vor Inkrafttreten der Richtlinie geschlossen wurden und die mit Unionsrecht in Einklang stehen, bleiben in Kraft, bis diese verändert, ersetzt oder aufgehoben werden (Art. 61). In Art. 62 ist ein umfangreiches Evaluationsverfahren vorgesehen. Die ersten Berichte müssen innerhalb von 4 Jahren nach Inkrafttreten vorgelegt werden. Innerhalb von 3 Jahren sind weitere Regelungen daraufhin zu überprüfen, ob sie angesichts der vorliegenden Richtlinie angepasst werden müssen. Gemäß Art. 63 Abs. 4 teilen die Mitgliedstaaten der EU-Kommission mit, welche Vorschriften sie zur Umsetzung der vorliegenden Richtlinie erlassen haben.

4 Bewertung

So zufrieden man als Datenschützer mit dem Trilog-Ergebnis zur EU-DSGVO sein kann, so wenig ist dies bei der Datenschutzrichtlinie für Polizei und Justiz gerechtfertigt. Zwar ist diese gegenüber dem bisher geltenden Rahmenbeschluss ein Fortschritt. Doch genügen die materiellen Regelungen in vieler Hinsicht nicht den hohen Anforderungen, die Eingriffe in das Grundrecht auf Datenschutz sowie in andere Grundrechte durch die Polizei und die Justiz stellen. Der Umstand, dass bei der europäischen Datenschutzreform die EU-DSGVO im Vordergrund stand, hat offenbar dazu geführt, dass bei der Richtlinie sich administrative Verarbeitungsinteressen keiner öffentlichen Kritik ausgesetzt waren und sich deshalb durchsetzen konnten.

Gemäß den Anforderungen des EuGH sind für informationelle Eingriffe „klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme“ nötig, die sich „auf das absolut Notwendige“ beschränkt[9]. Diesen Anforderungen genügt die Richtlinie selbst nicht. Dem muss aber das die Richtlinie umsetzende nationale Recht genügen.

[9] EuGH, U. v. 06.10.2015, Rn. 91, 92

4.1 Mangelhafte Betroffenentransparenz

Besonders defizitär sind die Ausnahmemöglichkeiten bei der Benachrichtigung über verdeckte Maßnahmen bzw. bei der Auskunftserteilung. Diese sehen pauschale Informationsverweigerungen vor, ohne dass eine Abwägung im Einzelfall erforderlich wäre, so in den Art. 13 Abs. 4, 15 Abs. 2. Ohne Kenntnis einer Datenverarbeitung ist es einem Betroffenen unmöglich, sein Grundrecht auf Datenschutz in der Praxis auszuüben. Gerade im Bereich von Strafverfolgung und Gefahrenabwehr haben Behörden umfassende Rechte zur heimlichen Datenerhebung. Umso wichtiger sind Benachrichtigungen und Auskunftsansprüche, um die Rechtsmäßigkeit der informationellen Eingriffe überprüfen (lassen) zu können. Die Ausnahmeregelung in Art. 13 Abs. 3 lit. b, 15 Abs. 1 lit. b „zur Gewährleistung, dass Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten nicht beeinträchtigt“ wird, eröffnet viele Möglichkeiten für willkürliche Informationsverweigerungen. Entsprechendes gilt für die Verweigerung „zum Schutz der öffentlichen Sicherheit“ (Art 13 Abs. 3 lit. c, 15 Abs. 1 lit. c). Die genannten Regelungen genügen nicht den Bestimmtheitsanforderungen, die sich aus Art. 8 Abs. 2 S. 1 EUGRCh ergeben, wo es heißt: „Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten ...“. Die Regelungen stellen nicht sicher, dass, wie im Grundrechtsbereich nötig, eine Abwägung im Einzelfall erfolgt.

Mit den Regelungen wird zudem die in Art. 47 EUGRCh zugesicherte Möglichkeit der Erlangung effektiven Rechtsschutzes beeinträchtigt, dessen Bedeutung der EuGH in der Safe-Harbor-Entscheidung vom 06.10.2015 hervorgehoben hat[10].

4.2 Auslandsübermittlung

Es ist äußerst fraglich, ob die Übermittlungsregelungen in Drittländer in den Art.35 ff. grundrechtskonform sind. Zwar enthält Art. 35 Abs. 3 eine salvatorische Abwägungsklausel: „Alle Regelungen dieses Kapitels sind so anzuwenden, dass sichergestellt wird, dass das durch diese Richtlinie garantierte Schutzniveau für den Einzelnen nicht untergraben wird.“ Die dann folgenden Normen greifen aber diesen Grundgedanken nur ungenügend wieder auf. Insbesondere bei den „Ausnahmen in spezifischen Situationen“ gemäß Art. 38 wird nicht in allen Fällen eine Abwägung gefordert[11].

Die materiellen Voraussetzungen für Datenübermittlungen ohne adäquaten Datenschutz bei den Empfängern sind teilweise äußerst niedrig und allgemein formuliert. Dies ist etwa der Fall bei der „strengen Erforderlichkeit“ für die Aufgabenerfüllung der übermittelnden Stelle in Art. 39 Abs. 1 lit. a[12].

Eine adäquate Interessenabwägung wird zudem dadurch in Frage gestellt, dass der Abwägungsvorgang ohne prozedurale Absicherungen regelmäßig durch die verantwortliche übermittelnde Stelle erfolgt, die mit der Übermittlung zumeist ein Eigeninteresse verfolgt. Nur in bestimmten Ausnahmefällen wird eine Informationspflicht gegenüber der Datenschutzaufsicht geregelt (Art. 37 Abs. 2), wobei eine Prüfung im Einzelfall nachschauend nur auf Initiative der Datenschutzaufsicht vorgesehen ist (Art. 37 Abs. 3, 38 Abs. 3). Eine wirksame präventive Sicherungswirkung kann ein solcher Mechanismus nicht entwickeln.

[10] C-362/14, Rn. 64, 95
[11] so explizit Art. 38 Abs. 2 mit Bezug auf Abs. 1 lit. a-c
[12] kritisch hierzu z. B. EuGH, U. v. 06.10.2015, Rn. 86 f.

5 Ausblick

Das deutsche Sicherheitsrecht dürfte weitgehend mit den materiell-rechtlichen Anforderungen der Richtlinie übereinstimmen.

Die Regelungen der Richtlinie zum technisch-organisatorischen Datenschutz genügen nicht den aktuellen Anforderungen. Angesichts der weitergehenden Regelungen in der EU-DSGVO sowie in einigen Landesgesetzen sollten sich die deutschen Gesetzgeber in Bund und Ländern weniger an der Richtlinie als an diesen Vorbildern orientieren.

Hinsichtlich der prozeduralen Regelungen zum Datenschutzbeauftragten, zur Datenschutzaufsicht und zum Rechtsschutz besteht auch in Deutschland großer Anpassungsbedarf. Bei diesem Anlass besteht die Möglichkeit, nicht nur die von der Richtlinie geforderten Minimalstandards einzuführen, sondern darüber hinausgehend Defizite der Richtlinie auf der nationalen Ebene zu beheben.

Die Regelungsmaterien des deutsche Polizeirechts werden nicht vollständig von der Richtlinie erfasst, sondern befassen sich auch mit Rechtsfragen, die unter die EU-DSGVO fallen. Dies ist z. B. bei der Fahndung nach Vermissten ohne Bezug auf das Vorliegen einer Straftat der Fall. Um insofern keine Unstimmigkeiten zu bewirken, sollte sich die Umsetzung im Polizeirecht im Zweifel an den jeweils grundrechtsfreundlicheren Regelungen der beiden europarechtlichen Instrumente orientieren.

Die Umsetzung der Richtlinie dürfte wegen der bestehenden europäischen Grundrechtsbindung weitgehend für den EuGH justiziabel sein. In der Safe-Harbor-Entscheidung vom 06.10.2015 hat der EuGH hohe materielle und prozedurale Anforderungen an Auslandsübermittlungen gestellt, insbesondere wenn diese ins Ausland ohne angemessenes Datenschutzniveau erfolgen[13]. Dies muss bei der Umsetzung berücksichtigt werden, wollen die Gesetzgeber auf nationaler Ebene nicht, wie schon oft in der Vergangenheit geschehen, gerichtlich korrigiert werden. Es ist davon auszugehen, dass es in den Mitgliedstaaten bei der grundrechtskonformen Umsetzung der Richtlinie massive Defizite geben wird. Dann liegen alle Hoffnungen beim EuGH, der dies korrigieren kann und muss.

6 Anhang zum vorstehenden Beitrag

Inhalt/Gliederung
Europäische Datenschutzrichtlinie für Polizei und Justiz

Erläuterungen:
1. Ziffer = Artikel in den Entwurfsfassungen
2. Ziffer in Klammern = voraussichtliche **Zählung der Artikel** in der Endfassung und **im vorstehenden Beitrag**
Text = Überschrift des Artikels/Kapitels/Abschnitts
3. Ziffer in Klammer = erläuternde Erwägungsgründe (EG) gemäß Entwurfsfassungen
4. Ziffer in Klammer hinter Schrägstrich = voraussichtliche Zählung der Erwägung (EG) in Endfassung

Kapitel 1 Allgemeine Bestimmungen

[13] C-362/14, Rn. 39, 73-78