Reform des europäischen Datenschutzrechts

Ein Überblick unter besonderer Berücksichtigung des Datenaustausches zwischen Polizei-, Strafjustiz- und Geheimdienstbehörden

Petra Beckerhoff

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

Data protection is one of today's most important challenges. Cross-border crime, terrorist risks, and new technologies all contribute to an increase in the collection and movement of personal data. This contribution first gives an overview of the content of the recently reformed European data protection law, i.e. the General Data Protection Regulation (GDPR). It also provides an analysis of Directive 2016/680, which regulates the specific protection of personal data in the prevention, investigation, detection and prosecution of criminal offences as well as the enforcement of criminal penalties. The article further outlines current projects and new developments regarding data transmission between intelligence agencies and prevention/prosecution authorities. It also focuses on the principle of limitation for the purpose of data use as well as the "compatibility" of operation purposes as rules for restricting data processing. The paper concludes by recommending the creation of harmonised and clear rules for data transmission with the intelligence agencies.

AUTHOR

Petra Beckerhoff

Rechtsanwältin in Münster (Westfalen)

CITE THIS ARTICLE

Beckerhoff, P. (2017). Reform des europäischen Datenschutzrechts : ein Überblick unter besonderer Berücksichtigung des Datenaustausches zwischen Polizei-, Strafjustiz- und Geheimdienstbehörden. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2017-010

Published in eucrim 2017, Vol. 12(2) pp 88 – 92

https://eucrim.eu

ISSN:

I. Einleitung

Die jüngste europäische Datenschutzreform besteht mit der ab dem 25. Mai 2018 in allen Mitgliedstaaten anzuwendenden EU-Datenschutzgrundverordnung (DS-GVO)[1] und der bis zum 6. Mai 2018 national umzusetzenden Richtlinie (EU) 2016/680[2] aus zwei Bestandteilen. Diese bilden im europäischen Datenschutzrecht die größte Neugestaltung seit der Datenschutzrichtlinie 95/46 (EG)[3] und legen erstmalig auch unionsweit einen Mindeststandard für den Datenschutz bei Polizei und Justiz fest.

Mit der Schaffung eines einheitlichen Schutzniveaus werden zugleich auch die Voraussetzungen für eine informationelle Zusammenarbeit zwischen den Strafverfolgungs- und Gefahrenabwehrbehörden geschaffen. Angesichts der aktuellen Herausforderungen durch die grenzüberschreitende Kriminalität und die terroristische Bedrohung wird ein Austausch relevanter Informationen verstärkt gefordert. Zudem können aufgrund von technischen Entwicklungen in zunehmend großem Umfang Daten verarbeitet, ausgetauscht und verknüpft werden. Allerdings ist ein Austausch von Informationen zwischen den Sicherheitsbehörden – einschließlich den Nachrichtendiensten – wegen der unterschiedlichen Aufgabenbereiche zumeist mit einer Änderung der Zweckbestimmung der Daten verbunden. Überdies handelt es sich oftmals um Daten, die mit eingriffsintensiven und aufgabenspezifischen Befugnissen und Methoden erhoben worden sind. Der Datenaustausch verlangt daher eine Balance zwischen den Interessen einer effektiven Strafverfolgung und Gefahrenabwehr einerseits und dem Schutz der Grund- und Menschenrechte des Einzelnen bei der Verarbeitung der ihn betreffenden Daten andererseits.

Mit dem vorliegenden Beitrag sollen neben den wesentlichen Inhalten der DS-GVO und der Richtlinie (RL) (EU) 2016/680 auch die aktuellen Bestrebungen im europäischen Datenschutz sowie die neueren Entwicklungen beim Ausbau und bei der Nutzung der Möglichkeiten des Informationsaustausches eingegangen werden. Beleuchtet wird dabei insbesondere der Zweckbindungsgrundsatz, dem bei der Zulässigkeit einer Zweckänderung von Informationen besondere Bedeutung zukommt.

II. Die Datenschutz-Grundverordnung (DS-GVO)

Die folgende Darstellung der grundlegenden Strukturen und wesentlichen Neuerungen der DS-GVO soll bereits mit Blick auf die gleichzeitig erlassene, in der öffentlichen Diskussion jedoch weniger beachteten RL (EU) 2016/680 zum Datenschutz bei Polizei und Justiz erfolgen (unten III.).

1. Zielsetzung

Unter Bezugnahme auf den der RL 95/46 (EG) zugrundeliegenden Harmonisierungsgedanken betont die neue Verordnung vor allem den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten. Die Schaffung eines unionsweit gleichmäßigen Schutzniveaus soll den freien Verkehr personenbezogener Daten im Binnenmarkt ermöglichen und der technisch und integrativ bedingten deutlichen Zunahme der Erhebung und des Austausches personenbezogener Daten gerecht werden.[4]

2. Anwendungsbereich

Die DS-GVO betrifft nach Art. 2 grundsätzlich die gesamte Verarbeitung personenbezogener Daten im Anwendungsbereich des Unionsrechts. Der Begriff der Verarbeitung von Daten schließt alle in Art. 4 Nr. 2 DS-GVO im Einzelnen genannten Datenverarbeitungsvorgänge ein, und damit neben der Ersterhebung auch die

für den Datenaustausch mögliche Abfrage und Übermittlung. Nicht in den Anwendungsbereich fallen Datenverarbeitungsvorgänge, die die nationale Sicherheit und die Gemeinsame Außen- und Sicherheitspolitik der Union betreffen.[5] Der Bereich der nationalen Sicherheit umfasst den Verteidigungsbereich und auch die Tätigkeiten der Inlands- und Auslandsgeheimdienste.[6] Mit der Ausnahmeregelung des Art. 2 III DS-GVO ist auch die Datenverarbeitung durch die EU und ihre Institutionen ausgenommen. Hierfür gilt zunächst weiterhin die VO (EG) 45/2001.[7]

Nicht in den Anwendungsbereich der DS-GVO einbezogen sind nach dessen Art. 2 II ferner Datenverarbeitungen zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich der Datenverarbeitung zum Schutz vor und zur Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum freien Verkehr dieser Daten. Hierfür gilt die neue RL (EU) 2016/680. Wie sich aus Erwägungsgrund (im Folgenden: EW) Nr. 19 der DS-GVO ergibt, soll die Abgrenzung nicht nach der institutionell organisatorischen Einordnung der Behörde, sondern nach dem Zweck erfolgen, zu dem die Datenverarbeitung erfolgt. Diese Betrachtung ist auch bei der Abgrenzung der einzelnen Datenverarbeitungsschritte heranzuziehen. In der Begründung zur Verordnung heißt es dazu, dass auch personenbezogene Daten, die von der Behörde nach der DS-GVO verarbeitet werden, dann der RL (EU) 2016/680 unterliegen sollten, wenn die Daten zu den in der RL genannten Zwecken verwendet werden.[8] Korrespondierende Ausführungen enthalten auch Art. 9 I 2, II der RL (EU) 2016/680 sowie die Erläuterungen in EW 34 der RL. Für einen Datenaustausch bedeutet dies, dass für die Ersterhebung der Daten durch die übermittelnde Behörde einerseits und die Verwendung der Daten durch den Empfänger andererseits auch unterschiedliche Rechtsgrundlagen maßgeblich sein können. Je nachdem, ob der jeweilige Datenvorgang zu den Zwecken der DS-GVO oder der RL (EU) 2016/680 erfolgt, beurteilt sich die Rechtmäßigkeit der Datenverarbeitung nach den Bestimmungen der DS-GVO oder den zur Umsetzung der Richtlinie ergangenen nationalen Bestimmungen. Als Beispiel kann der Abruf von Bankdaten zum Zwecke der Ermittlung, Aufdeckung oder Verfolgung von Straftaten genannt werden.

Die unmittelbar in den Mitgliedstaaten geltende Verordnung lässt den nationalen Gesetz-gebern durch Öffnungsklauseln einige Spielräume zur Konkretisierung und Regelung.[9] Diese betreffen beispielsweise die Rechtmäßigkeit von Datenverarbeitungen im öffentlichen Interesse und ihre Zweckbindung, die Verarbeitung besonderer Kategorien von Daten oder den Daten-schutzbeauftragten.[10]

3. Grundsätze der Datenverarbeitung

Der Katalog der Grundsätze, die jede Datenverarbeitung gemäß Art. 5 DS-GVO erfüllen muss, ist im Vergleich zur RL 95/46 um weitere unstreitige Datenschutzprinzipien, wie Vertraulichkeit und Rechenschaftspflicht, ergänzt worden. Der insbesondere für den Datenaustausch bedeutsame Zweckbindungsgrundsatz ist in Art. 5 I b) DS-GVO definiert. Danach müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Voraussetzungen für die Zulässigkeit eines Datenaustausches werden durch den Grundsatz der Vereinbarkeit der Zwecke von Ersterhebung und geänderter Nutzung normiert.

Konkretisierungen, aber auch Ausnahmetatbestände zur Zweckbindung finden sich fernerhin in den Bestimmungen zur Rechtmäßigkeit der Verarbeitung (Art. 6 III und IV DS-GVO), welche im EW 50 näher erläutert werden. Für den Fall der Vereinbarkeit von Erhebungs- und Weiterverarbeitungszweck sei, so EW 50 der Verordnung, keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Für die Beurteilung der Vereinbarkeit sieht Art. 6 IV DS-GVO eine nicht abschließende Auflistung maßgeblicher Kriterien vor. Zugleich folgt aus Art. 6 IV DS-GVO eine weitere Einschränkung: Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf

Unionsrecht oder dem Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, sollen die Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeitet werden dürfen. Die Verordnung sieht beim Schutz hochrangiger Interessen eine Zweckänderung somit grundsätzlich als gerechtfertigt an.

Die Verordnung zeigt damit bereits einige Aspekte der grundlegenden Problematik der Zulässigkeit von Zweckänderungen auf. Das Bundesverfassungsgericht hat in einer neueren Entscheidung zur Verfassungsmäßigkeit des Gesetzes für das Bundeskriminalamt das Kriterium der Vereinbarkeit durch das Prinzip der hypothetischen Datenneuerhebung ersetzt, womit die früheren Maßstäbe an eine Zweckänderung teilweise zurückgenommen werden.[11] Auch wenn an dieser Stelle nicht auf die Einzelheiten der Voraussetzungen einer Zweckänderung eingegangen werden kann, sollen einige Gesichtspunkte kurz aufgezeigt werden. Fraglich ist danach, welcher Maßstab für den Begriff der Vereinbarkeit gelten sollte; in Betracht kommt eine Entsprechung der Zweckbestimmung oder, wie es die DS-GVO nahelegt, eine Interessenabwägung. Eine Rolle können auch die Mittel und Methoden der Erlangung der Daten oder die Erhebungsvoraussetzungen spielen. Eine weitere Frage ist, ob eine Rechtsgrundlage für jeden Datenverarbeitungsschritt zu fordern ist. Ferner kann bereits der Konkretisierungs- bzw. Abstrahierungsgrad der ursprünglichen Zweckbestimmung ein entscheidendes Kriterium für das Vorliegen einer Zweckänderung sein. Auch der Zeitpunkt ist für die Beurteilung der Vereinbarkeit von Bedeutung.[12] Schließlich dürfte nach der deutschen höchstrichterlichen Entscheidung als Maßstab für die Zweckbindung das Verhältnis zwischen dem Kriterium der Vereinbarkeit und der Rechtsfigur der hypothetischen Datenneuerhebung eine gesonderte Betrachtung erfordern.

4. Wesentliche Neuerungen

Die wesentlichen Neuerungen der DS-GVO betreffen die Rechte des Betroffenen, technische und organisatorische Anforderungen an Datenschutz bzw. Datensicherheit, die Übermittlung von Daten an Drittstaaten sowie Aufsichts- und Sanktionsmaßnahmen. Darüber hinaus bringt die Verordnung Veränderungen beim Beschäftigten-Datenschutz und der Auftragsdatenverarbeitung.

Ein Anliegen der DS-GVO ist es, die Verarbeitung der Daten für den Betroffenen fair und transparent zu gestalten. Dazu ist der Umfang der Informationen, die dem Betroffenen nach Art. 13 und 14 DS-GVO im Vergleich zur RL 95/46 (EG) mitgeteilt werden müssen, erweitert worden. Zusammen mit dem Auskunftsrecht bilden die Informationspflichten schon zumeist rein tatsächlich die Voraussetzung dafür, die Rechtmäßigkeit der Datenverarbeitung überprüfen zu lassen und Rechte wie das Recht auf Berichtigung, Löschung Widerspruch und Beschwerde geltend machen zu können. Die DS-GVO enthält in Art. 12 Vorgaben über Aufbereitung der Information für den Betroffenen, die auch spezielle Vorgaben für an Kinder zu richtende Informationen beinhalten. Das auch als „Recht auf Vergessenwerden“ bezeichnete Löschungsrecht wird im Hinblick auf das Internet nach Art. 17 DS-GVO ausgeweitet und ein Recht auf Datenportabilität (Art. 20 DS-GVO) wird eingeführt.

Im Bereich der technischen und organisatorischen Anforderungen sind auf europäischer Ebene die Bestellung eines Datenschutzbeauftragten, eine Datenschutz-Folgenabschätzung, Zertifizierungs- sowie Melde- und Dokumentationspflichten statuiert.[13] Das technische Konzept der Privacy by Design und by Defaults wird geregelt.[14]

Der Datentransfer in Staaten außerhalb der EU folgt nach Art. 44 ff DS-GVO weiterhin dem Grundsatz der Angemessenheit, über den die Kommission entscheidet; er wird jedoch durch zwei weitere Bestimmungen

zur Möglichkeit der Datenübermittlung vorbehaltlich geeigneter Garantien und – als Ausnahmetatbestand konzipiert – derjenigen für den Fall berechtigter Interessen erweitert.

Überdies sind Aufgaben und Befugnisse der Aufsichtsbehörden überarbeitet worden. Für grenzüberschreitende Datenverarbeitungen gilt zukünftig das Prinzip einer einheitlichen Aufsichtsbehörde, das sog. One-Stop-Shop-Prinzip. Weitere Neuerungen betreffen Sanktions- und Haftungsbestimmungen.

III. Richtlinie (EU) 2016/680 zum Datenschutz bei Polizei und Justiz

Die Richtlinie (EU) 2016/680 entspricht hinsichtlich des Aufbaus und vieler Regelungsinhalte weitgehend der gleichzeitig verkündeten DS-GVO. Sie ersetzt den Rahmenbeschluss 2008/977/JI[15] des Rates und gilt im Unterschied zu diesem nicht nur für die grenzüber-schreitende, sondern auch für die innerstaatliche Datenverarbeitung.

1. Zielsetzung

Ziele der RL sind nach Art. 1 II die Grundrechte natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, zu schützen und gleichzeitig den ungehinderten Datenverkehr im Polizei- und Justizbereich zu erleichtern. Um jedoch ein hohes Schutzniveau zu gewährleisten, erhalten die Mitgliedstaaten nach Art 1 III der RL (EU) 2016/680 ausdrücklich die Möglichkeit, strengere Garantien für die Datenverarbeitung festzulegen, als sie in der Richtlinie vorgesehen sind, was zulasten einer Vollharmonisierung geht.

2. Anwendungsbereich

Der Anwendungsbereich wird durch den Gegenstand der Datenverarbeitung nach Art. 1 I RL (EU) 2016/ 680 bestimmt, durch den auch die Abgrenzung zur DS-GVO erfolgt. Wie die DS-GVO ist auch die Richtlinie nicht auf den Bereich der nationalen Sicherheit und auf die Institutionen der EU anwendbar, sodass die Datenverarbeitung durch die Nachrichtendienste sowie durch Europol und Eurojust ausgenommen sind. Für den Austausch mit Interpol soll die Richtlinie neben dem Gemeinsamen Standpunkt 2005/ 69/JI und dem Beschluss 2007/533/JI des Rates anwendbar sein.[16]

Im Unterschied zur DS-GVO differenziert die Richtlinie, dem spezifischen Schutzgedanken entsprechend, zwischen verschiedenen Datenkategorien, wie die des Verdächtigen, der Opfer oder Zeugen und den unterschiedlichen Grundlagen der Daten.

3. Grundsätze der Datenverarbeitung

Art. 4 I RL (EU) 2016/680 enthält, wie die DS-GVO, grundlegende Prinzipien für die Datenverarbeitung, zu denen auch der Grundsatz der Zweckbindung zählt. Art. 4 I b) RL (EU) 2016/680 knüpft die Datenverarbeitung zu anderen Zwecken, als zu denen sie erhoben worden sind, ebenfalls an die Vereinbarkeit der Zweckbestimmung von Datenerhebung und Datenverarbeitung. Die Bestimmungen der Richtlinie zur Zweckänderung gehen jedoch nicht so weit wie die der DS-GVO, was unter anderem dadurch begründet ist, dass die Richtlinie den Mitgliedstaaten Regelungsspielräume lässt. Art. 4 II RL (EU) 2016/680 sieht lediglich vor, dass für die Verarbeitung der Daten innerhalb der Zwecksetzung der Richtlinie eine Rechtsgrundlage besteht und die Datenverarbeitung für den neuen Zweck erforderlich und verhältnismäßig ist.

Für die Zweckänderung durch Datenübermittlung sieht Art. 9 III RL (EU) 2016/680 vor, dass besondere Bedingungen, die für die Datenverarbeitung gelten, auch vom Datenempfänger eingehalten werden sollen. Dies soll jedoch nach Art. 9 IV RL (EU) 2016/680 nur gelten, sofern die besonderen Bedingungen auch für entsprechende Datenübermittlungen im innerstaatlichen Recht vorgesehen sind und insoweit eine Gleichbehandlung gewährleistet ist.

4. Wesentliche Neuerungen

Die wesentlichen Neuerungen der Richtlinie sind im Kern denen der DS-GVO ähnlich. Dies gilt beispielsweise für die Informations- und Löschungspflichten, die Rechtsbehelfe sowie die Regelungen zum Datenschutzbeauftragten, zum technischen Datenschutz und zur Datenschutz-Folgenabschätzung. Entsprechungen zur DS-GVO bestehen auch bei der Datenübermittlung an Drittstaaten und den Kontrollmechanismen. Abweichungen erfolgen teilweise dem spezifischen Anwendungsbereich der RL entsprechend, um Ermittlungen nicht zu gefährden oder einem besonderen Schutzbedürfnis gegenüber den Ermittlungen gerecht zu werden.[17]

IV. Aktuelle Reformbestrebungen

Mit den jüngsten umfangreichen Reformen ist der Erneuerungsprozess nicht abgeschlossen. Bereits am 10. Januar 2017 hat die Kommission im Rahmen der Digitalen Binnenmarktstrategie ein weiteres Datenschutz-Reformpaket vorgelegt, das zeitgleich mit der DS-GVO ab dem 25. Mai 2018 anwendbar sein soll. Dieses beinhaltet einen Vorschlag für die Verarbeitung personenbezogener Daten durch die Organe und Institutionen der EU, der die derzeit geltende VO (EG) 45/2001 ersetzen soll.[18] Der Entwurf orientiert sich zwar an der DS-GVO, lässt neben speziellen anwendungstypischen Abweichungen aber auch Beschränkungen durch die EU-Institutionen zu.

Das Reformpaket sieht ferner eine Neuordnung der für die elektronische Kommunikation geltenden Datenschutz-Richtlinie 2002/58 (EG) vor.[19] Diese sogenannte E-Datenschutz-Richtlinie regelt die Verarbeitung personenbezogener Daten durch öffentlich zugängliche elektronische Kommunikationsdienste in der EU. Sie erfasst auch die Verarbeitung von Verkehrsdaten. Diese sind wiederum auch Gegenstand der äußerst streitigen sog. Vorratsdatenspeicherung.

Im Rahmen der Bewältigung technischer Herausforderungen plant die Kommission auch eine Initiative zum Aufbau einer europäischen Datenwirtschaft.[20] Durch die Initiative soll der freie grenzüberschreitende Datenverkehr in der EU ermöglicht werden, indem ungerechtfertigte nationale Beschränkungen, die nicht dem Grundrechtsschutz dienen, abgebaut werden und insbesondere die durch neue Datentechniken aufgeworfenen Zugangs-, Eigentums- und Haftungsfragen geklärt werden. Für den ungehinderten Datenfluss als Voraussetzung für die Grundfreiheiten des EU-Binnenmarktes soll ein sicherer Rechtsrahmen geschaffen werden, damit Daten über die gesamte Wertschöpfungskette hinweg für wissenschaftliche, gesellschaftliche und industrielle Prozesse genutzt werden können. Die Regelungen sollen auch nicht personenbezogene maschinen-generierte Daten umfassen und können einen Beitrag zur Industrie 4.0 leisten, bei der industrielle Produktionsprozesse mit moderner Informations- und Kommunikationstechnik vernetzt sind.[21]

Der europäische Datenschutz steht jedoch noch vor weiteren Herausforderungen. Vor dem Hintergrund terroristischer Bedrohungen regt die Europäische Kommission die Einrichtung eines sog. „Drehkreuzes für den Informationsaustausch“ an, um einen effektiven und zeitnahen Informationsaustausch auch zwischen den Strafverfolgungsstellen und den Nachrichtendiensten herzustellen.[22] Ein Austausch zwischen den nationalen Diensten findet in der derzeit außerhalb des EU-Rahmens bestehenden Gruppe für

Terrorismusbekämpfung (CTG) statt.[23] Eine Zusammenarbeit von Strafverfolgungsstellen und Nachrichtendiensten soll im Rahmen der geltenden EU-Verträge mit den zuständigen Mitgliedstaaten im Wege „praktischer Lösungen" erfolgen und bei Europol angesiedelt werden.[24] Aus Deutschland können Erfahrungen des Terrorismusabwehrzentrums in Berlin eingebracht werden.

Auf der Grundlage der seit dem 01. Mai 2017 geltenden neuen Europol-Verordnung VO (EU) 2016/794[25] sollen Europol und insbesondere das dort eingerichtete Europäische Zentrum zur Terrorismusbekämpfung weiter ausgebaut werden.[26] Die Europol-Verordnung enthält ebenfalls Datenschutzregelungen, insbesondere die Statuierung des Zweckbindungsgrundsatzes sowie bereichsspezifische Rechtssätze zur Zweckbestimmung der Informationsverarbeitung und zur Zusammenarbeit mit Eurojust und OLAF.

Eine neue Stufe der Zusammenarbeit bei der Strafverfolgung wird durch die geplante Errichtung einer Europäischen Staatsanwaltschaft erfolgen.[27] Der Europäische Staatsanwalt soll als unabhängiges Organ der Union für die Untersuchung, Verfolgung und Anklage von Straftaten zum Nachteil der finanziellen Interessen der Union und damit untrennbar verbundenen Tätigkeiten zuständig sein. Geplant sind eine Zentralstelle sowie die Einsetzung der delegierten europäischen Staatsanwälte, die in den Mitgliedstaaten angesiedelt sind. Für die Verarbeitung personenbezogener Daten enthält Kapitel VI des Verordnungsentwurfs umfangreiche bereichsspezifische Bestimmungen, die auch von einer Zweckbindung der Daten ausgehen.

V. Ausblick

Die nationalen Maßnahmen zur Anpassung des Datenschutzrechts an die DS-GVO und zur Umsetzung der RL (EU) 2016/ 680 haben in Deutschland mit einem entsprechenden Gesetzentwurf begonnen.[28] Es sollen jedoch noch weitere bereichsspezifische Regelungen folgen.

Angesichts der Vielzahl der geltenden Rechtsakte und dem unterschiedlichen Umfang nationaler Regelungskompetenzen für einen Datenaustausch zwischen den für die Strafverfolgung, die Gefahrenabwehr sowie die nationale Sicherheit zuständigen Behörden können die Kriterien für eine Zweckänderung ein wirksames Instrument für den Gleichlauf der Datenverarbeitung bilden. Anknüpfungspunkte sind der Grundsatz der Zweckbindung und der Maßstab der hypothetischen Datenneuerhebung. Insbesondere im Verhältnis von Strafverfolgung und nationaler Sicherheit können – angesichts dessen, dass die nationalen Sicherheitsbehörden aus dem Anwendungsbereich des europäischen Datenschutzrahmens fallen – diese Ansätze eine Möglichkeit bieten, die Datenersterhebungs- und Datenverwendungsbestimmungen anzugleichen. Überdies können einheitliche Anforderungen an eine Zweckänderung zu einer Begrenzung der Datenverknüpfungen der sog. Big-Data-Anwendungen führen. Bei diesen Prozessen sind ebenfalls personenbezogene Daten betroffen, deren Verwendung nicht nur durch das technisch Machbare begrenzt werden können. Insgesamt bleibt zu wünschen, dass weitere Schritte zur Harmonisierung des Datenschutzes erfolgen, die auch einheitliche und klare Regelungen für den notwendigen Datenaustausch zwischen den Nachrichten- und Sicherheitsdiensten festlegen.

---

1. ABl. (EU) L 119, 1 vom 4.5.2016.↩
2. ABL. (EU) L 119, 89 vom 4.5.2016.↩
3. ABl. (EU) L 281, 31 vom 23.11.1995.↩
4. Erwägungsgründe Nr. 5 und 9 der DS-GVO.↩
5. Erwägungsgrund Nr. 16 der DS-GVO.↩
6. BT-Drucks. 18/11325, S. 2, 74.↩
7. ABl. (EU) L 8, 1 vom 12.1.2001.↩
8. Erwägungsgrund Nr. 19 der DS-GVO.↩
9. Zu den einzelnen Öffnungsklauseln Kühling/Martini et al., *Die Datenschutz-Grundverordnung und das nationale Recht*, 2016.↩
10. Vgl. Art. 6 II, III; 9 IIa), IV; 37 IV, 88 DS-GVO.↩

11. BVerfG, Urt. vom 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 287, 292 (abrufbar unter: http://www.bverfg.de/e/rs20160420_1bvr096609.html [zuletzt abgerufen: 3.7.17]).↩
12. Es kommen der Zeitpunkt der Datenerhebung, der der Datenübermittlung oder der Moment der Datenverwendung in Betracht.↩
13. Vgl. Art. 37, 35, 42, 33, 30 DS-GVO.↩
14. Vgl. Art. 25 DS-GVO.↩
15. ABl. (EU) L 350, 60 vom 30.12.2008.↩
16. Erwägungsgrund Nr. 25 der RL (EU) 2016/680.↩
17. Vgl. die Regelungen der Art. 13 III, 15 RL (EU) 2016/680 einerseits und Art. 6 RL (EU) 2016/680 andererseits.↩
18. Europäische Kommission, COM (2017) 8 final; dazu Pressemitteilung vom 10.1.2017, IP/17/5.↩
19. Europäische Kommission, COM (2017) 10 final; dazu Pressemitteilung vom 10.1.2017 IP/2017/5.↩
20. Siehe die Mitteilung: Europäische Kommission > Vertretung in Deutschland > News >" Europäische Datenwirtschaft: EU-Kommission stellt Konzept für Daten-Binnenmarkt vor", abrufbar unter: https://ec.europa.eu/germany/news/europ%C3%A4ische-datenwirtschaft-eu-kommission-stellt-konzept-f%C3%BCr-daten-binnenmarkt-vor_de (zuletzt abgerufen: 3.7.17).↩
21. Siehe Europäische Kommission, COM(2017) 9 final.↩
22. Ratsdok. 12307/16, S. 17, 18.↩
23. Ratsdok. 12307/16, S. 14.↩
24. Ratsdok. 12307/16, S. 15, 18.↩
25. ABl. (EU) L 135, 53 vom 24.05.2016.↩
26. Ratsdok. 12307/16, S. 16, 17.↩
27. Zum Stand siehe News-Sektion in dieser Ausgabe.↩
28. BT-Drucks. 18/11325.↩

COPYRIGHT/DISCLAIMER
© 2018 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.
Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union