Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO, insbesondere in Bezug auf die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden

angenommen am 12. März 2019

INHALTSVERZEICHNIS

Der Europäische Datenschutzausschuss

gestützt auf Artikel 63 und Artikel 64 Absatz 2 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden „DSGVO“),

gestützt auf das EWR-Abkommen und insbesondere Anhang XI und Protokoll 37, zuletzt geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018,

gestützt auf Artikel 10 und Artikel 22 seiner Geschäftsordnung vom 25. Mai 2018 in der am 23. November 2018 geänderten Fassung,

in Erwägung nachstehender Gründe:

(1) Die wesentliche Aufgabe des Europäischen Datenschutzausschusses (EDSA, im Folgenden „der Ausschuss“) besteht darin, die kohärente Anwendung der Verordnung 2016/679 (im Folgenden „DSGVO“) im gesamten Europäischen Wirtschaftsraum sicherzustellen. Artikel 64 Absatz 2 der DSGVO sieht vor, dass jede Aufsichtsbehörde, der Vorsitz des Ausschuss oder die Kommission beantragen können, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten. Das Ziel dieser Stellungnahme ist es, eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat zu prüfen.

(2) Am 3. Dezember 2018 ersuchte die belgische Datenschutzbehörde beim Europäischen Datenschutzausschuss um eine Prüfung und Stellungnahme zum Zusammenspiel zwischen der DSGVO und der e-Datenschutz-Richtlinie, insbesondere mit Bezug auf die Zuständigkeit, die Aufgaben und die Befugnisse von Datenschutzbehörden.

(3) Die Stellungnahme des Ausschusses muss nach Artikel 64 Absatz 3 der DSGVO in Verbindung mit Artikel 10 Absatz 2 der Geschäftsordnung binnen acht Wochen ab dem ersten Werktag angenommen werden, nach dem der Vorsitz und die zuständige Aufsichtsbehörde entschieden haben, dass die Akte vollständig ist. Auf Beschluss des Vorsitzes kann diese Frist unter Berücksichtigung der Komplexität der Angelegenheit um weitere sechs Wochen verlängert werden -

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 ZUSAMMENFASSUNG DER FAKTEN

1. Am 3. Dezember 2018 ersuchte die belgische Datenschutzbehörde beim Europäischen Datenschutzausschuss um eine Prüfung und Stellungnahme zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie[1] und der DSGVO und legte folgende Fragen vor:

   a. Bezüglich der **Zuständigkeiten, Aufgaben und Befugnisse** der Datenschutzbehörden[2], ob
      i. Datenschutzbehörden berechtigt sind, ihre Zuständigkeiten, Aufgaben und Befugnisse in Bezug auf eine Verarbeitung auszuüben, die - zumindest in Bezug auf bestimmte Verarbeitungsvorgänge - in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt, oder nicht, und falls dies zutrifft, ob
      ii. Datenschutzbehörden bei der Ausübung ihrer Zuständigkeiten, Aufgaben und Befugnisse gemäß der DSGVO (etwa bei der Beurteilung der Rechtmäßigkeit der Verarbeitung) Bestimmungen der e-Datenschutz-Richtlinie und/oder ihrer nationalen Anwendungen berücksichtigen müssen, und wenn ja, inwieweit.
   b. Ob das Verfahren der Zusammenarbeit und das Kohärenzverfahren auf eine Verarbeitung, die - zumindest in Bezug auf bestimmte Verarbeitungsvorgänge - in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt, angewandt werden können oder sollten, sowie
   c. in welchem Umfang für die Verarbeitung **Bestimmungen sowohl der e-Datenschutz-Richtlinie als auch der DSGVO gelten können**, und ob dies die Antworten auf die Fragen 1 und 2 beeinflusst oder nicht.

2. Der Ausschuss ist der Auffassung, dass diese Fragen die allgemeine Anwendung der DSGVO betreffen, da die klare Notwendigkeit besteht, dass die Datenschutzbehörden die Grenzen ihrer Zuständigkeiten, Aufgaben und Befugnisse kohärent auslegen. Diese Klarstellung ist insbesondere nötig, um unter anderem eine kohärente Praxis gegenseitiger Amtshilfe nach Artikel 61 der DSGVO und gemeinsamer Maßnahmen nach Artikel 62 der DSGVO sicherzustellen.

3. Die vorliegende Stellungnahme bezieht sich nicht auf eine derartige Aufteilung der Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden nach dem Vorschlag für die e-Datenschutz-Verordnung.

[1] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2006/24/EG und die Richtlinie 2009/136/EG geänderten Fassung.

[2] Wie in den Artikeln 55 bis 58 der DSGVO festgelegt. In dieser Stellungnahme wird durchgängig der Begriff „Datenschutzbehörden“ (im Unterschied zu „Aufsichtsbehörden“) verwendet, um die in der DSGVO vorgesehenen „Aufsichtsbehörden“ eindeutig von anderen Arten von Aufsichtsbehörden zu unterscheiden, etwa den in der Richtlinie 2002/58/EG angeführten nationalen Regulierungsbehörden.

2 RECHTLICHER RAHMEN

2.1 Einschlägige Bestimmungen der DSGVO

4. Nach Artikel 2 Absatz 1 gilt die DSGVO für *„die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen*."
Gemäß Artikel 2 Absatz 2 der DSGVO findet die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten

> *„a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,*
>
> *b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,*
>
> *c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,*
>
> *d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit".*

5. Artikel 5 enthält unter dem Titel „Grundsätze für die Verarbeitung personenbezogener Daten" die für jede Verarbeitung personenbezogener Daten geltenden Grundsätze einschließlich der Vorgabe, dass die Verarbeitung personenbezogener Daten rechtmäßig und nach Treu und Glauben erfolgen muss.[3] In Artikel 6 sind die Bedingungen für eine rechtmäßige Verarbeitung personenbezogener Daten festgelegt, darunter die Einwilligung der betroffenen Person. In Artikel 7 werden die Bedingungen für eine gültige Einwilligung im Sinne der DSGVO näher ausgeführt.[4]

6. In Artikel 51 Absatz 1 wird das rechtliche Mandat der Datenschutzbehörden dargelegt, das in der Überwachung der Anwendung der DSGVO besteht und darauf abzielt, die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung zu schützen und den freien Verkehr personenbezogener Daten in der Union zu ermöglichen. Die Artikel 55, 57 und 58 enthalten nähere Ausführungen zu den Zuständigkeiten, Aufgaben und Befugnissen der einzelnen Datenschutzbehörden. In Kapitel VII der DSGVO werden unter dem Titel „Zusammenarbeit und Kohärenz" die verschiedenen Formen der Zusammenarbeit aufgeführt, durch die die Datenschutzbehörden zu einer kohärenten Anwendung der DSGVO beitragen sollen.

7. Artikel 94 bestimmt unter dem Titel „Aufhebung der Richtlinie 95/46/EG" Folgendes:

> *„(1) Die Richtlinie 95/46/EG wird mit Wirkung vom 25. Mai 2018 aufgehoben.*
>
> *(2) Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für*

[3] Siehe auch Erwägungsgrund 39 der DSGVO („*Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. […]*").
[4] Siehe die Leitlinien der Artikel-29-Datenschutzgruppe in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP259 rev.01, gebilligt durch den Europäischen Datenschutzausschuss am 25. Mai 2018.

den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss."

8. Artikel 95 sieht unter dem Titel „Verhältnis zur Richtlinie 2002/58/EG" Folgendes vor:

„Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen."

9. Erwägungsgrund 173 der DSGVO legt Folgendes fest:

„(173) Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten."

2.2 Relevante Bestimmungen der Rahmenrichtlinie

10. Artikel 2 Buchstabe g der Rahmenrichtlinie[5] definiert eine „nationale Regulierungsbehörde" als

„eine oder mehrere Stellen, die von einem Mitgliedstaat mit einer der in dieser Richtlinie und den Einzelrichtlinien festgelegten Regulierungsaufgaben beauftragt werden".

11. Artikel 2 Buchstabe l der Rahmenrichtlinie legt fest, dass

mit „Einzelrichtlinien" „die Richtlinie 2002/20/EG (Genehmigungsrichtlinie), die Richtlinie 2002/19/EG (Zugangsrichtlinie), die Richtlinie 2002/22/EG (Universaldienstrichtlinie) und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)" gemeint sind.

12. In Artikel 3 Absatz 1 der Rahmenrichtlinie wird Folgendes festgelegt:

„Die Mitgliedstaaten sorgen dafür, dass alle den nationalen Regulierungsbehörden mit dieser Richtlinie und den Einzelrichtlinien übertragenen Aufgaben von einer zuständigen Stelle wahrgenommen werden".

2.3 Maßgebliche Bestimmungen der e-Datenschutz-Richtlinie

13. In Artikel 1 Absatz 2 der e-Datenschutz-Richtlinie ist festgelegt, dass

[5] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie).

die „Bestimmungen dieser Richtlinie (...) eine Detaillierung und Ergänzung der Richtlinie 2016/679/EG im Hinblick auf die in Absatz 1 genannten Zwecke" darstellen. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt."[6]

14. In Artikel 2 Buchstabe f der e-Datenschutz-Richtlinie ist festgelegt, dass

der Begriff *„‚Einwilligung' eines Nutzers oder Teilnehmers die Einwilligung der betroffenen Person im Sinne von [Verordnung (EU) 2016/679]"* bezeichnet.

15. Nach Artikel 15 Absatz 2 der e-Datenschutz-Richtlinie gelten

die *„Bestimmungen des [Kapitels VIII der Verordnung (EU) 2016/679] über Rechtsbehelfe, Haftung und Sanktionen (...) im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte*".

16. Gemäß Artikel 15 Absatz 3 der e-Datenschutz-Richtlinie nimmt

„[der Europäische Datenschutzausschuss] ... auch die in [Artikel 70 der Verordnung (EU) 2016/679] festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr".

17. In Artikel 15a wird unter dem Titel „Anwendung und Durchsetzung" Folgendes vorgeschrieben:

„(1) Die Mitgliedstaaten legen fest, welche Sanktionen, gegebenenfalls einschließlich strafrechtlicher Sanktionen, bei einem Verstoß gegen die innerstaatlichen Vorschriften zur Umsetzung dieser Richtlinie zu verhängen sind, und treffen die zu deren Durchsetzung erforderlichen Maßnahmen. […]

(2) Unbeschadet etwaiger gerichtlicher Rechtsbehelfe stellen die Mitgliedstaaten sicher, dass die zuständige nationale Behörde und gegebenenfalls andere nationale Stellen befugt sind, die Einstellung der in Absatz 1 genannten Verstöße anzuordnen.

(3) Die Mitgliedstaaten stellen sicher, dass die zuständigen nationalen Regulierungsbehörden und gegebenenfalls andere nationale Stellen über die erforderlichen Untersuchungsbefugnisse und Mittel verfügen, einschließlich der Befugnis, sämtliche zweckdienliche Informationen zu erlangen, die sie benötigen, um die Einhaltung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften zu überwachen und durchzusetzen.

(4) Zur Gewährleistung einer wirksamen grenzübergreifenden Koordinierung der Durchsetzung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften und zur Schaffung harmonisierter Bedingungen für die Erbringung von Diensten, mit denen ein grenzüberschreitender Datenfluss verbunden ist, können die zuständigen nationalen Regulierungsbehörden Maßnahmen erlassen.

[6] Gemäß Artikel 94 Absatz 2 der DSGVO wurden sämtliche Verweise auf die Richtlinie 95/46 in der e-Datenschutz-Richtlinie durch „[Verordnung (EU) 2016/679]" ersetzt, und Verweise auf die „durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten" wurden durch „[Europäischer Datenschutzausschuss]" ersetzt.

Die nationalen Regulierungsbehörden übermitteln der Kommission rechtzeitig vor dem Erlass solcher Maßnahmen eine Zusammenfassung der Gründe für ein Tätigwerden, der geplanten Maßnahmen und der vorgeschlagenen Vorgehensweise. Die Kommission kann hierzu nach Prüfung der Informationen und Konsultationen mit der ENISA und dem [Europäischen Datenschutzausschuss] Kommentare oder Empfehlungen abgeben, insbesondere um sicherzustellen, dass die vorgesehenen Maßnahmen das ordnungsmäßige Funktionieren des Binnenmarktes nicht beeinträchtigen. Die nationalen Regulierungsbehörden tragen den Kommentaren oder Empfehlungen der Kommission weitestgehend Rechnung, wenn sie die Maßnahmen beschließen."

18. In Erwägungsgrund 10 der e-Datenschutz-Richtlinie ist Folgendes festgelegt:

> *„Im Bereich der elektronischen Kommunikation gilt die [Verordnung (EU) 2016/679] vor allem für alle Fragen des Schutzes der Grundrechte und Grundfreiheiten, die von der vorliegenden Richtlinie nicht spezifisch erfasst werden, einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen. Die [Verordnung (EU) 2016/679] gilt für nicht öffentliche Kommunikationsdienste.*"

3 ANWENDUNGSBEREICH DIESER STELLUNGNAHME

19. Ziel der DSGVO ist es, die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten zu schützen und den freien Verkehr personenbezogener Daten in der Union sicherzustellen.[7] Zur Erreichung dieses Ziels sind in der DSGVO gemeinsame Regeln zur Datenverarbeitung festgelegt, um in der Union einen gleichmäßigen effektiven Schutz personenbezogener Daten zu gewährleisten und Unterschiede zu beseitigen, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten. Die Regeln sollen ein ausgewogenes Verhältnis zwischen dem (potenziellen) Nutzen der Datenverarbeitung und den (potenziellen) Nachteilen sicherstellen.

20. Die e-Datenschutz-Richtlinie zielt auf die Harmonisierung der Vorschriften der Mitgliedstaaten ab, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.[8] Die e-Datenschutz-Richtlinie soll somit gewährleisten, dass die in den Artikeln 7 und 8 der Charta niedergelegten Rechte uneingeschränkt geachtet werden. In diesem Sinne zielt die e-Datenschutz-Richtlinie auf eine „Detaillierung und Ergänzung" der Bestimmungen der DSGVO in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation ab.[9]

21. Die dem Ausschuss vorgebrachten Fragen beschränken sich auf Verarbeitungen, die in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fallen. Um

[7] Artikel 1 der DSGVO.
[8] Artikel 1 Absatz 1 der e-Datenschutz-Richtlinie.
[9] Artikel 1 Absätze 1 und 2 der e-Datenschutz-Richtlinie, zu lesen im Lichte von Artikel 94 Absatz 2 der DSGVO.

den Anwendungsbereich dieser Stellungnahme weiter zu verdeutlichen, wird in den folgenden Abschnitten geklärt,

- wo es kein Zusammenspiel zwischen der DSGVO und der e-Datenschutz-Richtlinie gibt, weil die betreffende Angelegenheit nicht in den Anwendungsbereich der DSGVO fällt,
- wo es kein Zusammenspiel zwischen der DSGVO und der e-Datenschutz-Richtlinie gibt, weil die betreffende Angelegenheit nicht in den Anwendungsbereich der e-Datenschutz-Richtlinie fällt, und
- wo ein Zusammenspiel zwischen der DSGVO und der e-Datenschutz-Richtlinie besteht, weil die betreffende Verarbeitung in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt.

3.1 Nicht in den Anwendungsbereich der DSGVO fallende Angelegenheiten

22. Grundsätzlich gilt die DSGVO unabhängig von der verwendeten Technologie für alle Formen der Verarbeitung personenbezogener Daten.[10] Die DSGVO gilt nicht, wenn

- keine personenbezogenen Daten verarbeitet werden (z. B. sind eine Rufnummer eines automatischen Kundendienstes einer juristischen Person oder die IP-Adresse eines digitalen Kopiergeräts in einem Firmennetzwerk keine personenbezogenen Daten),
- die Tätigkeiten unter Berücksichtigung von Artikel 2 Absätze 2 und 3 der DSGVO nicht in den sachlichen Anwendungsbereich der DSGVO fallen, oder
- die Tätigkeiten nicht in den räumlichen Anwendungsbereich der DSGVO fallen.[11]

3.2 Nicht in den Anwendungsbereich der e-Datenschutz-Richtlinie fallende Angelegenheiten

23. Eine Besonderheit der e-Datenschutz-Richtlinie besteht darin, dass zwei der darin enthaltenen Bestimmungen einen weiteren Anwendungsbereich als die übrigen Bestimmungen haben, für welche der Anwendungsbereich auf die Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen beschränkt ist. Um feststellen zu können, ob eine Tätigkeit in den sachlichen Anwendungsbereich der e-Datenschutz-Richtlinie fällt oder nicht, gilt es daher die zwei in den nachfolgenden Abschnitten behandelten Fragen zu klären.

3.2.1 Der allgemeine sachliche Anwendungsbereich der e-Datenschutz-Richtlinie

24. Gemäß Artikel 3 gilt die e-Datenschutz-Richtlinie für „*die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen*“.

25. Insofern befasst sich die e-Datenschutz-Richtlinie in erster Linie mit öffentlich zugänglichen elektronischen Kommunikationsdiensten und öffentlichen Kommunikationsnetzen.[12]

[10] Siehe auch Erwägungsgrund 46 der e-Datenschutz-Richtlinie.
[11] Artikel 3 der DSGVO. Siehe dazu die Leitlinien 3/2018 des Europäischen Datenschutzausschusses zum räumlichen Anwendungsbereich der DSGVO (Artikel 3) vom 16. November 2018.

Der Kodex für die elektronische Kommunikation[13] sieht eine Anwendbarkeit auf Dienste vor, die elektronischen Kommunikationsdiensten in der Funktionsweise gleichwertig sind.

26. Für die Zwecke ihres allgemeinen sachlichen Anwendungsbereichs gilt die e-Datenschutz-Richtlinie, wenn alle folgenden Bedingungen erfüllt sind:

- Es gibt einen elektronischen Kommunikationsdienst[14];
- dieser Dienst wird über ein elektronisches Kommunikationsnetz[15] angeboten;
- der Dienst und das Netz sind öffentlich zugänglich[16];
- der Dienst und das Netz werden in der Europäischen Union angeboten.

27. Tätigkeiten, die nicht sämtlichen vorgenannten Kriterien genügen, fallen allgemein nicht in den Anwendungsbereich der e-Datenschutz-Richtlinie.

Beispiele:

Ein Firmennetzwerk, auf das nur Mitarbeiter für berufliche Zwecke Zugriff haben, ist kein „öffentlich zugänglicher" elektronischer Kommunikationsdienst. Folglich fällt die Übertragung von Standortdaten über ein solches Netz nicht in den sachlichen Anwendungsbereich der e-Datenschutz-Richtlinie. [17]

---

[12] Arbeitsunterlage der Kommissionsdienststellen, Ex-post-REFIT-Evaluierung der e-Datenschutz-Richtlinie 2002/58/EG, Bericht COM SWD(2017)005, S. 20; Bericht an die Kommission „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (e-Datenschutz-Richtlinie: Bewertung der Umsetzung, der Wirksamkeit und der Vereinbarkeit mit der vorgeschlagenen Datenschutzverordnung), SMART 2013/0071, S. 24 ff.

[13] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation.

[14] In Artikel 2 Buchstabe d der e-Datenschutz-Richtlinie wird ausgeführt, dass „Nachricht" jede Information bezeichnet, „die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird", wovon die Rundfunkdienste ausgenommen werden, die – theoretisch – eine unbegrenzte Teilnehmerzahl erreichen können. Der Begriff „elektronischer Kommunikationsdienst" wird gegenwärtig in Artikel 2 Buchstabe d der Rahmenrichtlinie bestimmt, soll aber ab dem 21. Dezember 2020 durch Artikel 2 Absatz 4 des Kodex für die elektronische Kommunikation definiert werden.

[15] Der Begriff „elektronisches Kommunikationsnetz" wird gegenwärtig in Artikel 2 Buchstabe d der Rahmenrichtlinie bestimmt, soll aber ab dem 21. Dezember 2020 durch Artikel 2 Absatz 1 des Kodex für die elektronische Kommunikation definiert werden.

[16] Ein Dienst für die Öffentlichkeit ist ein allen Mitgliedern der Öffentlichkeit auf der gleichen Grundlage zugänglicher Dienst und nicht nur ein im öffentlichen Besitz befindlicher Dienst. Vergleiche EDSB, Stellungnahme 5/2016, Vorläufige Stellungnahme des EDSB zur Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG), S. 14 f. sowie die Mitteilung der Kommission an das Europäische Parlament und den Rat über den Stand der Umsetzung der Richtlinie 90/388/EWG über den Wettbewerb auf dem Markt für Telekommunikationsdienste (KOM(95) 113 endg. vom 4.4.1995, S. 15.

[17] Arbeitsunterlage der Kommissionsdienststellen, Ex-post-REFIT-Evaluierung der e-Datenschutz-Richtlinie 2002/58/EG, Bericht COM SWD(2017)005, S. 21, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0005&from=EN; Bericht an die Kommission „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (e-Datenschutz-Richtlinie: Bewertung der Umsetzung, der Wirksamkeit und der Vereinbarkeit mit der vorgeschlagenen Datenschutzverordnung), SMART 2013/0071, S. 14, https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

Ein Dienst zur Synchronisierung von Uhren sendet über ein elektronisches Kommunikationsnetz an alle Uhren, die sein Synchronisierungsprotokoll befolgen (unbestimmte Empfängerzahl), ein Signal. Es handelt sich bei diesem Dienst im vorliegenden Kontext um einen Rundfunkdienst, der ebenfalls nicht in den sachlichen Anwendungsbereich der e-Datenschutz-Richtlinie fallen würde.

3.2.2 Der erweiterte sachliche Anwendungsbereich von Artikel 5 Absatz 3 und Artikel 13 der e-Datenschutz-Richtlinie

28. Das übergreifende Ziel der e-Datenschutz-Richtlinie besteht in der Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten der Öffentlichkeit bei der Nutzung von elektronischen Kommunikationsnetzen.[18] Im Lichte dieser Zielsetzung gelten Artikel 5 Absatz 3 und Artikel 13 der e-Datenschutz-Richtlinie für Anbieter elektronischer Kommunikationsdienste wie auch für Betreiber von Websites (z. B. für Cookies) oder andere Unternehmen (z. B. für Direktmarketing).[19]

Beispiele:

Suchmaschinendienste, die Cookies auf dem Gerät eines Benutzers speichern und darauf zugreifen, fallen in den erweiterten sachlichen Anwendungsbereich von Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie.[20]

Vom Betreiber einer Website zum Zweck des Direktmarketings versendete unerwünschte elektronische Post fällt ebenfalls in den erweiterten sachlichen Anwendungsbereich von Artikel 13 der e-Datenschutz-Richtlinie.[21]

3.3 Angelegenheiten, die in den sachlichen Anwendungsbereich sowohl der e-Datenschutz-Richtlinie als auch der DSGVO fallen

29. Es gibt viele Beispiele für Verarbeitungstätigkeiten, die in den sachlichen Anwendungsbereich sowohl der e-Datenschutz-Richtlinie als auch der DSGVO fallen. Ein eindeutiges Beispiel ist die Verwendung von Cookies. In ihrer Stellungnahme zur Werbung auf Basis von Behavioural Targeting hat die Artikel-29-Datenschutzgruppe dazu Folgendes festgestellt:

> *„Wenn die erhobenen Informationen als Ergebnis der Platzierung eines Cookies oder ähnlichen Instruments und des Abrufens der Informationen als personenbezogene Daten*

[18] Artikel 1 Absatz 1 der e-Datenschutz-Richtlinie sieht Folgendes vor: *„Diese Richtlinie sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.“*

[19] Artikel-29-Datenschutzgruppe, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting vom 22. Juni 2010, WP 171, Abschnitt 3.2.1, S. 10; Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148), Abschnitt 4.1.3., S. 13 f; Bericht an die Kommission „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation“ (e-Datenschutz-Richtlinie: Bewertung der Umsetzung, der Wirksamkeit und der Vereinbarkeit mit der vorgeschlagenen Datenschutzverordnung), SMART 2013/0071, S. 9.

[20] Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148), Abschnitt 4.1.3., S. 13 f.

[21] Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148), Abschnitt 4.1.3., S. 13 f.

*angesehen werden können, findet **zusätzlich** zu Artikel 5 Absatz 3 auch die Richtlinie 95/46/EG Anwendung.*“[22]

30. Der Gerichtshof der Europäischen Union (EuGH) hat in seiner Rechtsprechung bestätigt, dass eine Verarbeitung zugleich in den sachlichen Anwendungsbereich sowohl der e-Datenschutz-Richtlinie als auch der DSGVO fallen kann. In der Rechtssache *Wirtschaftsakademie*[23] wendete der EuGH die Richtlinie 95/46/EG unbeschadet der Tatsache an, dass die zugrundeliegende Verarbeitung auch Verarbeitungsvorgänge umfasste, die in den Anwendungsbereich der e-Datenschutz-Richtlinie fallen. In der anhängigen Rechtssache *Fashion ID* hat der Generalanwalt die Ansicht geäußert, dass in einem Fall, der Social Plugins und Cookies betrifft, beide Vorschriften anwendbar sind.[24]

31. Ungeachtet der am 25. Mai 2018 erfolgten Ersetzung der Richtlinie 95/46/EG durch die DSGVO sind die Analysen des EuGH und der Artikel-29-Datenschutzgruppe, wonach beide Rechtsakte gleichzeitig gelten können, weiterhin relevant. In Erwägungsgrund 30 der DSGVO wird der Begriff „Online-Kennungen“ in einer Weise näher definiert, die die Auslegung stützt, dass die Verarbeitung personenbezogener Daten in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fallen kann:

> *„Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.*“

32. Besonders bemerkenswert ist, dass die Begriffe „IP-Adressen“ und „Cookie-Kennungen“ im Erwägungsgrund 30 erwähnt werden, in dem erklärt wird, dass IP-Adressen und Cookie-Kennungen mit „eindeutigen Kennungen“ und anderen beim Server eingehenden Informationen kombiniert werden können, um Profile von natürlichen Personen zu erstellen.

33. Anders ausgedrückt bezieht sich die DSGVO bei der Klärung ihres eigenen sachlichen Anwendungsbereichs (d.h. des Begriffs „personenbezogene Daten“) selbst ausdrücklich auf Verarbeitungstätigkeiten, die zumindest teilweise auch in den sachlichen Anwendungsbereich der e-Datenschutz-Richtlinie fallen.

34. Ein weiteres Beispiel für eine Tätigkeit, die in den sachlichen Anwendungsbereich sowohl der e-Datenschutz-Richtlinie als auch der DSGVO fällt, ist die Kundenbeziehung zwischen einem Anbieter elektronischer Kommunikationsdienste und einer natürlichen Person, die diese Dienste nutzt, welche einerseits die Verarbeitung personenbezogener Daten über die Kunden betreffen und andererseits bestimmten Regeln unterliegen (beispielsweise zu Teilnehmerverzeichnissen,

---

[22] Artikel-29-Datenschutzgruppe, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting vom 22. Juni 2010, WP 171, S. 11. Siehe auch die Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148), Abschnitt 4.1.3., S. 13 f.

[23] EuGH, C-210/16, 5. Juni 2018, C-210/16, ECLI:EU:C:2018:388. Vgl. insbesondere die Randnummern 33 und 34.

[24] Schlussanträge des Generalanwalts Bobek in der Rechtssache Fashion ID, C-40/17, 19. Dezember 2018, ECLI:EU:C:2018:1039. Vgl. insbesondere die Randnummern 111 bis 115.

Einzelgebührennachweisen und der Anzeige der Rufnummer des Anrufers). Durch elektronische Kommunikationsdienste erzeugte Verkehrs- und Standortdaten können ebenfalls die Verarbeitung personenbezogener Daten betreffen, insofern sie sich auf natürliche Personen beziehen.

35. Schließlich wird in Artikel 95 der DSGVO und in Erwägungsgrund 173 der DSGVO das Verhältnis von Lex specialis und Lex generalis zwischen der DSGVO und der e-Datenschutz-Richtlinie bestätigt, wobei Artikel 95 bestimmt, dass die DSGVO natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Europäischen Union keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der e-Datenschutz-Richtlinie festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

***

36. Ziel dieser Stellungnahme ist es, Klarheit über die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden zu schaffen und Empfehlungen für Fälle auszusprechen, die in den sachlichen Anwendungsbereich sowohl der e-Datenschutz-Richtlinie als auch der DSGVO fallen, wie in den vorangehenden Abschnitten kurz dargestellt. In den folgenden Abschnitten werden Beispiele für das Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO angeführt und die Beziehungen zwischen verschiedenen Vorschriften beschrieben.

4 ZUSAMMENSPIEL ZWISCHEN DER E-DATENSCHUTZ-RICHTLINIE UND DER DSGVO

37. Obwohl sich die e-Datenschutz-Richtlinie und die DSGVO überschneiden, führt dies nicht notwendigerweise zu einem Konflikt zwischen diesen beiden Rechtsvorschriften. Zum einen wird dies deutlich, wenn man die verschiedenen Bestimmungen nebeneinander liest, und zum anderen bestimmt Artikel 1 Absatz 2 der e-Datenschutz-Richtlinie ausdrücklich, dass *„die Bestimmungen dieser Richtlinie (...) eine Detaillierung und Ergänzung der Richtlinie 95/46/EG*“ darstellen.[25] Für ein angemessenes Verständnis des Zusammenspiels zwischen der e-Datenschutz-Richtlinie und der DSGVO ist es zunächst notwendig, die Bedeutung von Artikel 1 Absatz 2 der e-Datenschutz-Richtlinie zu klären. Im Anschluss gilt es die Bedeutung und die Auswirkungen von Artikel 95 der DSGVO zu klären.

4.1 „Detaillierung“

38. Verschiedene Bestimmungen der e-Datenschutz-Richtlinie stellen *„Detaillierungen*“ der Bestimmungen der DSGVO in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation dar. Nach dem Grundsatz *lex specialis derogat legi generali* haben besondere Bestimmungen in den Situationen, die sie spezifisch regeln sollen, Vorrang vor allgemeinen Bestimmungen.[26] In Situationen, in denen die e-Datenschutz-Richtlinie Vorschriften der

[25] Artikel 94 Absatz 2 der DSGVO besagt, dass Verweise auf die aufgehobene Richtlinie 95/46 als Verweise auf die DSGVO gelten.

[26] Urteil des EuGH in den verbundenen Rechtssachen T-60/06 RENV II und T-62/06 RENV II, 22. April 2016, ECLI:EU:T:2016:233, Randnummer 81.

DSGVO „detailliert“ (d. h. spezifischer ausführt), müssen die (spezifischen) Bestimmungen der e-Datenschutz-Richtlinie als „*Lex specialis*“ Vorrang vor den (allgemeineren) Bestimmungen der DSGVO haben.[27] Gleichwohl gelten für Datenverarbeitungen, die nicht spezifisch durch die e-Datenschutz-Richtlinie geregelt sind (oder für die die e-Datenschutz-Richtlinie keine „spezifische Vorschrift“ enthält), weiter die Bestimmungen der DSGVO.

39. Ein Beispiel für die „Detaillierung“ von Bestimmungen der DSGVO durch die e-Datenschutz-Richtlinie findet sich in Artikel 6 der e-Datenschutz-Richtlinie, der die Verarbeitung sogenannter Verkehrsdaten betrifft. Für gewöhnlich kann die Verarbeitung personenbezogener Daten auf Basis jedes in Artikel 6 der DSGVO erwähnten rechtmäßigen Grundes gerechtfertigt sein. Gleichwohl kann ein Anbieter eines elektronischen Kommunikationsdienstes den gesamten Umfang der in Artikel 6 der DSGVO vorgesehenen rechtmäßigen Gründe nicht auf die Verarbeitung von Verkehrsdaten anwenden, weil Artikel 6 der e-Datenschutz-Richtlinie die Voraussetzungen, unter denen Verkehrsdaten einschließlich personenbezogener Daten verarbeitet werden dürfen, ausdrücklich einschränkt. In diesem Fall haben die spezifischeren Bestimmungen der e-Datenschutz-Richtlinie Vorrang vor den allgemeineren Bestimmungen der DSGVO. Artikel 6 der e-Datenschutz-Richtlinie beschneidet indessen nicht die Anwendung anderer Bestimmungen der DSGVO, wie der Rechte der betroffenen Person. Er negiert auch nicht das Erfordernis, dass personenbezogene Daten auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden müssen (Artikel 5 Absatz 1 Buchstabe a der DSGVO).

40. Eine vergleichbare Situation ergibt sich bezüglich Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie, insofern es sich bei im Gerät des Endnutzers gespeicherten Informationen um personenbezogene Daten handelt. Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie sieht vor, dass die Speicherung von Informationen oder der Zugriff auf bereits gespeicherte Informationen im Endgerät eines Teilnehmers oder Nutzers in der Regel der vorherigen Zustimmung bedarf.[28] In dem Maße, in dem es sich bei den im Gerät des Endnutzers gespeicherten Informationen um personenbezogene Daten handelt, muss Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie gegenüber Artikel 6 der DSGVO bezüglich des Speicherns dieser Informationen oder des Zugriffs darauf Vorrang haben. Vergleichbar ist das Ergebnis auch beim Zusammenspiel zwischen Artikel 6 der DSGVO und den Artikeln 9 und 13 der e-Datenschutz-Richtlinie. Dort, wo diese Artikel die Zustimmung zu den darin beschriebenen spezifischen Tätigkeiten erfordern, kann sich der für die Verarbeitung Verantwortliche nicht auf den ganzen Umfang der in Artikel 6 der DSGVO vorgesehenen rechtmäßigen Gründe berufen.

41. Aus dem Prinzip der „*Lex specialis*“ folgt, dass es eine Ausnahme von der allgemeinen Regel nur dann geben darf, wenn das Gesetz zu einem bestimmten Gegenstand auch eine spezielle Regel enthält. Die den Fall betreffenden Fakten müssen sorgfältig analysiert werden, um befinden zu können, wie weit die Ausnahme geht; dies gilt insbesondere für Fälle, in denen Daten zahlreichen unterschiedlichen Verarbeitungen unterzogen werden, sei es parallel oder aber fortlaufend.

---

[27] Artikel-29-Datenschutzgruppe, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting vom 22. Juni 2010, WP 171, S. 12.

[28] Nach Artikel 5 Absatz 3 können Informationen im Endgerät eines Teilnehmers oder Nutzers auch dann gespeichert oder kann auf diese zugegriffen werden, wenn es sich um eine technische Speicherung oder einen Zugang handelt, deren alleiniger Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist, oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Beispiel:
Ein Datenhändler erstellt Profile auf der Grundlage von Informationen über das Browsing-Verhalten von Einzelpersonen, die unter Verwendung von Cookies gesammelt wurden, aber auch personenbezogene Daten enthalten können, die über andere Quellen bezogen wurden (z. B. „Geschäftspartner"). In diesem Fall unterliegt ein Teil der fraglichen Verarbeitung (nämlich das Platzieren und Lesen von Cookies) der nationalen Bestimmung, mit der Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie umgesetzt wurde. Die nachfolgende Verarbeitung personenbezogener Daten, die durch Cookies erhoben wurden, muss außerdem eine Rechtsgrundlage nach Artikel 6 der DSGVO haben, um rechtmäßig zu sein.[29]

4.2 „Ergänzung"

42. Die e-Datenschutz-Richtlinie enthält außerdem Bestimmungen zur „*Ergänzung*" der Bestimmungen der DSGVO in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation. Zahlreiche Bestimmungen zielen beispielsweise auf den Schutz von „Teilnehmern" oder „Nutzern" eines öffentlich zugänglichen elektronischen Kommunikationsdienstes ab. Bei den Teilnehmern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann es sich um natürliche oder juristische Personen handeln. Indem sie die DSGVO ergänzt, schützt die e-Datenschutz-Richtlinie nicht nur die Grundrechte natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, sondern auch die berechtigten Interessen juristischer Personen.[30]

4.3 Die Bedeutung von Artikel 95 der DSGVO

43. Laut Artikel 95 der DSGVO erlegt die DSGVO „*natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.*" (Hervorhebung hinzugefügt).

44. Artikel 95 zielt daher darauf ab, für die Verarbeitung Verantwortliche, die andernfalls einem vergleichbaren, aber nicht völlig gleichen Verwaltungsaufwand ausgesetzt wären, vor unnötigem Verwaltungsaufwand zu bewahren. Ein Beispiel, das die Anwendung dieses Artikels veranschaulicht, hat mit der Meldepflicht für Verletzungen des Schutzes personenbezogener Daten zu tun, die sowohl von der e-Datenschutz-Richtlinie[31] als auch der DSGVO[32] auferlegt wird. Beide Rechtsvorschriften enthalten die Auflagen, die Sicherheit zu gewährleisten und etwaige Verletzungen des Schutzes personenbezogener Daten der zuständigen nationalen Behörde bzw. der Datenschutzbehörde zu melden. Diese Auflagen gelten parallel nach beiden Rechtsvorschriften entsprechend ihrem jeweiligen Anwendungsbereich. Es ist klar, dass eine doppelte (d.h. zum einen nach der DSGVO und zum anderen nach der e-Datenschutz-Richtlinie bestehende) Meldepflicht einen zusätzlichen Aufwand ohne unmittelbaren offenkundigen Nutzen für den Datenschutz bedeuten würde. Nach

[29] Die Datenschutzbehörden können Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie nur durchsetzen, wenn ihnen das nationale Recht eine solche Zuständigkeit verleiht. Sie sollten gleichwohl berücksichtigen, dass die Verarbeitung insgesamt mit spezifischen Tätigkeiten einhergeht, für die die Union durch ihre Rechtsetzung einen zusätzlichen Schutz schaffen wollte, um eine Untergrabung dieses Schutzes zu verhindern.
[30] Erwägungsgrund 12 der e-Datenschutz-Richtlinie.
[31] Artikel 4 der e-Datenschutz-Richtlinie.
[32] Artikel 32 bis 34 der DSGVO.

Artikel 95 der DSGVO sind Anbieter von elektronischen Kommunikationsdiensten, die eine Verletzung des Schutzes personenbezogener Daten in Befolgung des geltenden nationalen e-Datenschutz-Rechts gemeldet haben, nicht verpflichtet, die Datenschutzbehörden nach Artikel 33 der DSGVO über dieselbe Verletzung zu benachrichtigen.

4.4 Koexistenz

45. In den Fällen, in denen besondere Bestimmungen existieren, die einen bestimmten Verarbeitungsvorgang oder eine Reihe von Vorgängen regeln, sollten die besonderen Bestimmungen Anwendung finden (*Lex specialis*), und in allen anderen Fällen (d. h. wenn keine besonderen Bestimmungen einen bestimmten Verarbeitungsvorgang oder eine Reihe von Vorgängen regeln) gilt die allgemeine Regelung (*Lex generalis*).

46. In Erwägungsgrund 173 wird bestätigt, dass die DSGVO bezüglich der Verarbeitung personenbezogener Daten, für die die spezifischen Auflagen der e-Datenschutz-Richtlinie nicht gelten, weiter Anwendung findet:

> *„Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates bestimmten Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen“*.[33]

47. In Erwägungsgrund 173 der DSGVO wird wiederholt, was bereits in Erwägungsgrund 10 der e-Datenschutz-Richtlinie gesagt wird, der Folgendes bestimmt: *„Im Bereich der elektronischen Kommunikation gilt die [Verordnung (EU) 2016/679] vor allem für alle Fragen des Schutzes der Grundrechte und Grundfreiheiten, die von der vorliegenden Richtlinie nicht spezifisch erfasst werden, einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen*.“

48. Beispielsweise muss ein Anbieter eines öffentlichen Kommunikationsnetzes oder öffentlich zugänglichen Kommunikationsdienstes bei der Verarbeitung von Daten, die für die Gebührenabrechnung und die Bezahlung von Zusammenschaltungen erforderlich sind, alle nationalen Vorschriften einhalten, durch die Artikel 6 Absatz 2 der e-Datenschutz-Richtlinie umgesetzt wird. Aufgrund des Fehlens spezifischer Bestimmungen zum elektronischen Datenschutz (etwa zum Auskunftsrecht) finden die Bestimmungen der DSGVO Anwendung. Entsprechend wird in Erwägungsgrund 32 der e-Datenschutz-Richtlinie bestätigt, dass in Fällen, in denen der Betreiber eines elektronischen Kommunikationsdienstes oder eines Dienstes mit Zusatznutzen die für die Bereitstellung dieser Dienste erforderliche Verarbeitung personenbezogener Daten an eine andere Stelle weiter vergibt, diese Weitervergabe und die anschließende Datenverarbeitung in vollem Umfang den Anforderungen in Bezug auf die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter im Sinne der DSGVO entsprechen müssen.

***

[33] Weiter heißt es in Erwägungsgrund 173: „Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten.“ Diese Überprüfung ist noch im Gange.

49. In den vorstehenden Abschnitten wurde dargelegt, wie die Bestimmungen der e-Datenschutz-Richtlinie und der DSGVO in Fällen zusammenwirken, in denen die Verarbeitung in den Anwendungsbereich beider Rechtsvorschriften fällt. Die folgenden Abschnitte werden sich mit Fragen befassen, die hinsichtlich der Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden an den Ausschuss herangetragen wurden, wobei auf Fälle Bezug genommen wird, die zumindest teilweise in den Anwendungsbereich der e-Datenschutz-Richtlinie fallen.

5 ZUSTÄNDIGKEITEN, AUFGABEN UND BEFUGNISSE VON DATENSCHUTZBEHÖRDEN

50. Die belgische Aufsichtsbehörde hat zwei Fragen bezüglich der Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden – wie in den Artikeln 55 bis 58 der DSGVO ausgeführt – an den Ausschuss gerichtet, die folgendermaßen umschrieben werden können:

- Schränkt allein schon die Tatsache, dass die Verarbeitung personenbezogener Daten in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt, die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden nach der DSGVO ein? Gibt es mit anderen Worten einen Teilsatz von Datenverarbeitungsvorgängen, den sie nicht berücksichtigen müssen, und wenn ja, in welchen Fällen?
- Müssen Datenschutzbehörden bei der Ausübung ihrer in der DSGVO festgelegten Zuständigkeiten, Aufgaben und Befugnisse (etwa bei der Beurteilung der Rechtmäßigkeit der Verarbeitung) die Bestimmungen der e-Datenschutz-Richtlinie berücksichtigen und wenn ja, inwieweit? Anders ausgedrückt: Sollten Verstöße gegen nationale e-Datenschutz-Vorschriften bei der Beurteilung der Einhaltung der DSGVO berücksichtigt oder außer Acht gelassen werden, und wenn ja, unter welchen Umständen?

51. Vorab sei angemerkt, dass die Mitgliedstaaten gehalten sind, die volle Wirksamkeit des Unionsrechts zu gewährleisten, indem sie insbesondere für geeignete Durchsetzungsmechanismen sorgen. Diese Pflicht beruht auf dem Grundsatz der loyalen Zusammenarbeit gemäß Artikel 4 Absatz 3 EUV.[34] In den folgenden Abschnitten werden kurz die Durchsetzungsbestimmungen der DSGVO bzw. der e-Datenschutz-Richtlinie und ihr Zusammenspiel beschrieben.

5.1 Durchsetzung der DSGVO

52. Die DSGVO sieht die Durchsetzung ihrer Bestimmungen durch unabhängige Datenschutzbehörden vor. Diesbezüglich ist auch anzumerken, dass Artikel 8 der Charta der Grundrechte der Europäischen Union vorsieht, dass die Verarbeitung personenbezogener Daten von einer unabhängigen Stelle überwacht werden muss:

[34] Artikel 4 Absatz 3 EUV sieht vor: *„Nach dem Grundsatz der loyalen Zusammenarbeit achten und unterstützen sich die Union und die Mitgliedstaaten gegenseitig bei der Erfüllung der Aufgaben, die sich aus den Verträgen ergeben. Die Mitgliedstaaten ergreifen alle geeigneten Maßnahmen allgemeiner oder besonderer Art zur Erfüllung der Verpflichtungen, die sich aus den Verträgen oder den Handlungen der Organe der Union ergeben. Die Mitgliedstaaten unterstützen die Union bei der Erfüllung ihrer Aufgabe und unterlassen alle Maßnahmen, die die Verwirklichung der Ziele der Union gefährden könnten.“*

*„**Artikel 8 – Schutz personenbezogener Daten***

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

*(3) Die Einhaltung **dieser** Vorschriften wird **von einer unabhängigen Stelle überwacht**.*

53. Den Datenschutzbehörden wird diesbezüglich das in Artikel 51 Absatz 1 DSGVO festgelegte rechtliche Mandat übertragen, die Anwendung der DSGVO zu überwachen, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird.

54. Die DSGVO sieht diesbezüglich gleichwohl eine Ausnahme sowie eine Möglichkeit vor, durch die dieses Mandat eingeschränkt wird:

- Die Verarbeitung personenbezogener Daten fällt nicht in die Zuständigkeit der Aufsichtsbehörden, wenn sie von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommen wird (Artikel 55 Absatz 3 DSGVO);
- für die Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, können die Mitgliedstaaten Abweichungen oder Ausnahmen unter anderem von Kapitel VI (Unabhängige Aufsichtsbehörden) und Kapitel VII (Zusammenarbeit und Kohärenz) der DSGVO vorsehen (Artikel 85 DSGVO).

Außerdem können die Befugnisse von Datenschutzbehörden in Übereinstimmung mit Artikel 58 Absatz 6 DSGVO erweitert und diese Datenschutzbehörden namentlich ermächtigt werden, gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen zu verhängen, falls ein Mitgliedstaat dies in seiner nationalen Gesetzgebung vorsieht (Artikel 83 Absatz 7 DSGVO).

Insofern sie Ausnahmen von der allgemeinen Regel darstellen, sind diese Bestimmungen eng auszulegen.

55. In den Fällen, in denen die DSGVO Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden einschränkt oder Abweichungen zulässt, tut sie dies ausdrücklich. Auch schließt die DSGVO Datenschutzbehörden in keiner Weise von der Ausübung ihrer Zuständigkeiten, Aufgaben und Befugnisse in Bezug auf die Verarbeitung aus, insofern diese in den sachlichen Anwendungsbereich der DSGVO fällt. Daher stellt sich die Frage, ob das Unionsrecht eine Einschränkung der allgemeinen Zuständigkeiten der Datenschutzbehörden in den Fällen vorgesehen oder zugelassen hat, in denen für die betreffende Verarbeitung Bestimmungen der e-Datenschutz-Richtlinie gelten.

5.2 Durchsetzung der e-Datenschutz-Richtlinie

56. Die Durchsetzung der e-Datenschutz-Richtlinie hängt eng mit der Rahmenrichtlinie[35] zusammen, die in Artikel 3 Absatz 1 vorschreibt, dass die „*Mitgliedstaaten (...) dafür (sorgen), dass alle den nationalen Regulierungsbehörden mit dieser Richtlinie und den Einzelrichtlinien übertragenen Aufgaben von einer zuständigen Stelle wahrgenommen werden*[36].“

57. Artikel 2 Buchstabe g der Rahmenrichtlinie definiert eine „nationale Regulierungsbehörde“ als

> *„eine oder mehrere Stellen, die von einem Mitgliedstaat mit einer der in dieser Richtlinie und den Einzelrichtlinien festgelegten Regulierungsaufgaben beauftragt werden.*“

58. Die Mitgliedstaaten haben verschiedene Wege gewählt, um die Aufgabe der Durchsetzung nationaler e-Datenschutz-Vorschriften an eine oder mehrere Stellen zu übertragen.[37] Diese Bandbreite verschiedener Ansätze ist möglich, weil die e-Datenschutz-Richtlinie lediglich einige allgemeine Ziele vorgibt, die die Mitgliedstaaten in dieser Angelegenheit erreichen müssen.

59. Die e-Datenschutz-Richtlinie schreibt nicht vor, dass nur eine einzige nationale Stelle für die Durchsetzung ihrer Bestimmungen zuständig sein muss. Tatsächlich sieht Artikel 15a der e-Datenschutz-Richtlinie ausdrücklich vor, dass mehr als nur eine nationale Stelle dafür zuständig sein kann, ihre Bestimmungen durchzusetzen. Artikel 15a sieht außerdem vor, dass die Mitgliedstaaten die Richtlinie anzuwenden und durchzusetzen haben und zu diesem Zweck unter anderem Sanktionen festlegen, die Befugnis zur Anordnung der Einstellung von Verstößen erteilen sowie Untersuchungsbefugnisse und Mittel bereitstellen müssen:

> *„(1) Die Mitgliedstaaten legen fest, welche Sanktionen, gegebenenfalls einschließlich strafrechtlicher Sanktionen, bei einem Verstoß gegen die innerstaatlichen Vorschriften zur Umsetzung dieser Richtlinie zu verhängen sind, und treffen die zu deren Durchsetzung erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein und können für den gesamten Zeitraum einer Verletzung angewendet werden, auch wenn die Verletzung in der Folge abgestellt wurde. Die Mitgliedstaaten teilen der Kommission diese Vorschriften bis zum 25. Mai 2011 mit und melden ihr unverzüglich etwaige spätere Änderungen, die diese Vorschriften betreffen.*

---

[35] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), in der geänderten Fassung.

[36] Artikel 2 Buchstabe l der Rahmenrichtlinie stellt klar, dass sich der Begriff „Einzelrichtlinien“ auf „*die Richtlinie 2002/20/EG (Genehmigungsrichtlinie), die Richtlinie 2002/19/EG (Zugangsrichtlinie), die Richtlinie 2002/22/EG (Universaldienstrichtlinie) und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)*“ bezieht.

[37] Bericht an die Kommission „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation“ (e-Datenschutz-Richtlinie: Bewertung der Umsetzung, der Wirksamkeit und der Vereinbarkeit mit der vorgeschlagenen Datenschutzverordnung), SMART 2013/0071, S. 33 ff.

(2) Unbeschadet etwaiger gerichtlicher Rechtsbehelfe stellen die Mitgliedstaaten sicher, dass die zuständige nationale Behörde ***und gegebenenfalls andere nationale Stellen*** *befugt sind, die Einstellung der in Absatz 1 genannten Verstöße anzuordnen.*

(3) Die Mitgliedstaaten stellen sicher, dass die zuständigen nationalen Regulierungsbehörden ***und gegebenenfalls andere nationale Stellen*** *über die erforderlichen Untersuchungsbefugnisse und Mittel verfügen, einschließlich der Befugnis, sämtliche zweckdienliche Informationen zu erlangen, die sie benötigen, um die Einhaltung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften zu überwachen und durchzusetzen.*

(4) Zur Gewährleistung einer wirksamen grenzübergreifenden Koordinierung der Durchsetzung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften und zur Schaffung harmonisierter Bedingungen für die Erbringung von Diensten, mit denen ein grenzüberschreitender Datenfluss verbunden ist, können die zuständigen nationalen Regulierungsbehörden Maßnahmen erlassen."

60. Zusätzlich enthält Artikel 15 Absatz 2 der e-Datenschutz-Richtlinie eine Bestimmung, die auf die Bestimmungen der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen Bezug nimmt und nunmehr als Bezugnahme auf die DSGVO zu lesen ist:

> *„Die Bestimmungen des Kapitels III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte."*

61. Artikel 15 Absatz 3 der e-Datenschutz-Richtlinie bestimmt ferner Folgendes:

> *„Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt auch die in Artikel 30 jener Richtlinie festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr."*[38]

5.3 Durchsetzung bei Überschneidungen von DSGVO und e-Datenschutz-Richtlinie

62. Die e-Datenschutz-Richtlinie ist eine Detaillierung und Ergänzung der DSGVO und bezieht sich darüber hinaus auf deren Bestimmungen über Rechtsbehelfe, Haftung und Sanktionen (Artikel 15 Absatz 2 der e-Datenschutz-Richtlinie gelesen im Lichte von Artikel 94 DSGVO).

---

[38] Artikel 15 Absatz 3 der e-Datenschutz-Richtlinie sieht vor: *„Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt auch die in Artikel 30 jener Richtlinie festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr*."
Artikel 94 Absatz 2 der DSGVO besagt: *„Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss."*
Folglich muss Artikel 30 der Richtlinie 95/46 als Bezugnahme auf die betreffenden Abschnitte von Artikel 70 der DSGVO (Aufgaben des Ausschusses) ausgelegt werden.

5.3.1 Frage 1: Sind bestimmte Datenverarbeitungsvorgänge für Datenschutzbehörden „tabu“?

- *Schränkt allein schon die Tatsache, dass die Verarbeitung personenbezogener Daten in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt, die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden nach der DSGVO ein? Gibt es mit anderen Worten einen Teilsatz von Verarbeitungsvorgängen, den sie nicht berücksichtigen sollten, und falls zutreffend, welche Verarbeitungsvorgänge sollten ausgenommen werden?*

63. Nach der DSGVO müssen die Mitgliedstaaten eine oder mehrere Aufsichtsbehörden einsetzen. Mitgliedstaaten können dieselbe Behörde mit der Zuständigkeit ausgestattet haben, die nationale Umsetzung der e-Datenschutz-Richtlinie (teilweise) durchzusetzen, aber sie können sich auch für eine oder mehrere andere Behörden entschieden haben, beispielsweise eine nationale Regulierungsbehörde für das Fernmeldewesen, eine Verbraucherschutzorganisation oder ein Ministerium.

64. Die e-Datenschutz-Richtlinie belässt den Mitgliedstaaten die Flexibilität, darüber zu entscheiden, welcher Behörde oder Stelle sie ihre Durchsetzung anvertrauen wollen.

65. Während die e-Datenschutz-Richtlinie auf die Bestimmungen der DSGVO bezüglich der Rechtsbehelfe, Haftung und Sanktionen eingeht (Artikel 15 Absatz 2 der e-Datenschutz-Richtlinie), werden in Artikel 15a Absatz 1 der e-Datenschutz-Richtlinie die Bestimmungen zur „Umsetzung und Durchsetzung“ der e-Datenschutz-Richtlinie ausgeführt. So bestimmt Artikel 15a Absatz 1 beispielsweise Folgendes: „*Die Mitgliedstaaten legen fest, welche Sanktionen, gegebenenfalls einschließlich strafrechtlicher Sanktionen, bei einem Verstoß gegen die innerstaatlichen Vorschriften zur Umsetzung dieser Richtlinie zu verhängen sind, und treffen die zu deren Durchsetzung erforderlichen Maßnahmen (...)“.* Insofern stellt die e-Datenschutz-Richtlinie die Sanktionen ausdrücklich dem Ermessen der Mitgliedstaaten anheim, und Artikel 15 Absatz 2 greift nicht in den Ermessensspielraum ein, der den Mitgliedstaaten bei der Durchsetzung gewährt wird (d. h. bei der Festlegung, wer die Bestimmungen der e-Datenschutz-Richtlinie durchzusetzen hat).[39]

66. Falls die Zuständigkeit für die Durchsetzung der e-Datenschutz-Richtlinie durch das nationale Recht auf die Datenschutzbehörde übertragen wurde, sollten auch die Befugnisse und Aufgaben der Datenschutzbehörde in Bezug auf die Durchsetzung der e-Datenschutz-Richtlinie durch das nationale Recht festgelegt werden. Die Datenschutzbehörde kann sich nicht automatisch auf die in der DSGVO vorgesehenen Aufgaben und Befugnisse stützen, um die nationalen e-Datenschutz-Vorschriften durchzusetzen, da diese Aufgaben und Befugnisse aus der DSGVO an deren Durchsetzung gebunden sind. Die nationale Gesetzgebung kann Aufgaben und Befugnisse zuweisen, die durch die DSGVO inspiriert sind, aber sie kann der Datenschutzbehörde für die Durchsetzung der nationalen e-Datenschutz-Vorschriften gemäß Artikel 15a der e-Datenschutz-Richtlinie auch andere Aufgaben und Befugnisse zuweisen.

[39] Es wird darauf hingewiesen, dass Artikel 15a Absatz 1 der e-Datenschutz-Richtlinie durch die Richtlinie 2009/136/EG (d. h. durch eine Änderung der e-Datenschutz-Richtlinie) eingeführt wurde.

67. Ein etwaiges Ermessen besteht nur innerhalb der Grenzen der Erfordernisse und Beschränkungen, die in höheren Vorschriften festgeschrieben sind. Artikel 8 Absatz 3 der Charta schreibt die Überwachung der Einhaltung der Datenschutzvorschriften durch eine unabhängige Behörde vor.[40]

68. Wenn die Verarbeitung personenbezogener Daten in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt, haben die Datenschutzbehörden nur dann die Zuständigkeit, Teilsätze der Verarbeitung zu untersuchen, die durch nationale Vorschriften zur Umsetzung der e-Datenschutz-Richtlinie geregelt sind, wenn das nationale Gesetz ihnen diese Zuständigkeit überträgt. Gleichwohl bleibt die Zuständigkeit von Datenschutzbehörden nach der DSGVO in Bezug auf Verarbeitungsvorgänge, die keinen speziellen Regeln der e-Datenschutz-Richtlinie unterliegen, in jedem Fall unbeschnitten. Diese Abgrenzung kann durch die nationale Gesetzgebung zur Umsetzung der e-Datenschutz-Richtlinie modifiziert werden (z. B. durch die Erweiterung des sachlichen Anwendungsbereichs über die Erfordernisse der e-Datenschutz-Richtlinie hinaus und die Übertragung der ausschließlichen Zuständigkeit für die betreffende Bestimmung an die nationale Regulierungsbehörde).

69. Die Datenschutzbehörden sind für die Durchsetzung der DSGVO zuständig. Durch die bloße Tatsache, dass ein Teilsatz der Verarbeitung in den Anwendungsbereich der e-Datenschutz-Richtlinie fällt, wird die Zuständigkeit von Datenschutzbehörden nach der DSGVO nicht eingeschränkt.

70. Falls einer anderen Stelle als der Datenschutzbehörde die ausschließliche Zuständigkeit übertragen wurde, bestimmt das nationale Verfahrensrecht, was zu geschehen hat, wenn betroffene Personen bei der Datenschutzbehörde Beschwerde einreichen, beispielsweise über die Verarbeitung personenbezogener Daten in Form von Verkehrs- oder Standortdaten, über unerwünschte elektronische Nachrichten oder das Sammeln von Daten durch Cookies, ohne sich zugleich über einen (etwaigen) Verstoß gegen die DSGVO zu beschweren.

5.3.2 Frage 2: Sind nationale e-Datenschutz-Bestimmungen „tabu“?

- *Müssen Datenschutzbehörden bei der Ausübung ihrer in der DSGVO festgelegten Zuständigkeiten, Aufgaben und Befugnisse (etwa bei der Beurteilung der Rechtmäßigkeit der Verarbeitung) die Bestimmungen der e-Datenschutz-Richtlinie berücksichtigen und wenn ja, inwieweit? Anders ausgedrückt: Sollten Verstöße gegen nationale e-Datenschutz-Vorschriften bei der Beurteilung der Einhaltung der DSGVO berücksichtigt oder außer Acht gelassen werden, und wenn ja, unter welchen Umständen??*

71. Ein Beispiel veranschaulicht den Unterschied zur ersten Frage: Ein Datenhändler erstellt Profile auf der Grundlage von Informationen, die aus zwei unterschiedlichen Quellen stammen. Die erste Quelle besteht aus unter Verwendung von Cookie-Kennungen und/oder anderen Gerätekennungen gesammelten Daten über das Nutzungsverhalten von Personen im Internet. Die zweite Quelle

[40] Das Erfordernis der Unabhängigkeit ist durch die einschlägige Rechtsprechung des EuGH zu Artikel 28 der Richtlinie 95/46 geklärt worden, siehe z. B. Urteil vom 9. März 2010, C-518/07 (Kommission gegen Deutschland), Randnummer 17 und folgende, Urteil vom 16. Oktober 2012, C-614/10 (Kommission gegen Österreich), Randnummer 36 und folgende, Urteil vom 6. Oktober 2015, C-362/14 („Sicherer Hafen“), Randnummer 41 und folgende, Urteil vom 21. Dezember 2016, C-203/15 und C698/15 (Tele2/Watson), Randnummer 123.

besteht aus Daten, die über Geschäftspartner bezogen wurden, welche Daten über Teilnehmer an Preisausschreiben oder Rückvergütungsprogrammen weitergeben.

72. Die Erstellung der Profile von Personen auf der Basis personenbezogener Daten fällt generell in den Anwendungsbereich der DSGVO und damit in die Zuständigkeit der Datenschutzbehörden. Inwieweit müssen Datenschutzbehörden bei der Beurteilung der Einhaltung der DSGVO spezifische Vorschriften, im vorliegenden Fall nationale e-Datenschutz-Vorschriften, berücksichtigen, wenn bei einer Datenschutzbehörde eine Beschwerde über die Erstellung von Profilen durch den Datenvermittler eingeht?

73. Es ist anzumerken, dass die e-Datenschutz-Richtlinie ein spezifisches Beispiel für eine Rechtsvorschrift ist, die bestimmte Datenkategorien, bei denen es sich um personenbezogene Daten handeln kann, besonders schützt. Andere Rechtsvorschriften gewähren ebenfalls bestimmten Arten von Daten, die personenbezogene Daten sein können, aus verschiedenen Gründen (z. B. aufgrund des Kontexts der Verarbeitung, der Art der Daten oder der Risiken für betroffene Personen) besonderen Schutz.[41]

74. Die Mitgliedstaaten sind verpflichtet, eine oder mehrere Behörden für die Aufsicht über die Einhaltung der nationalen Rechtsvorschriften zur Umsetzung der e-Datenschutz-Richtlinie einzusetzen, und diese Behörde(n) ist (sind) dann für die Durchsetzung dieser Rechtsvorschriften zuständig. Die nationalen Rechtsvorschriften zur Umsetzung der e-Datenschutz-Richtlinie gelten für bestimmte Datenverarbeitungsvorgänge, die unter die e-Datenschutz-Richtlinie fallen, beispielsweise für einen Verarbeitungsvorgang, der die Speicherung von und den Zugriff auf Informationen auf dem Gerät des Endnutzers umfasst.

75. Datenschutzbehörden können die Bestimmungen (des nationalen Rechts zur Anwendung) der e-Datenschutz-Richtlinie als solche nicht durchsetzen, wenn sie ihre Zuständigkeiten nach der DSGVO ausüben, es sei denn, das nationale Recht überträgt ihnen diese Zuständigkeit. Gleichwohl kann, wie bereits angemerkt, eine Verarbeitung personenbezogener Daten, die Vorgänge einschließt, welche in den sachlichen Anwendungsbereich der e-Datenschutz-Richtlinie fallen, zusätzliche Aspekte umfassen, für die die e-Datenschutz-Richtlinie keine „spezielle Vorschrift“ enthält. So enthält etwa Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie eine spezielle Vorschrift für das Speichern von Informationen oder den Zugriff auf bereits gespeicherte Informationen auf dem Gerät eines Endnutzers. Er enthält aber keine spezielle Vorschrift für vorhergehende oder nachfolgende Verarbeitungstätigkeiten (etwa die Speicherung und Analyse von Daten über die Web-Browsing-Aktivitäten zum Zweck von Werbung auf Basis von Behavioural Targeting oder zu

[41] Ein Beispiel findet sich im Finanzsektor: Einen besonderen Schutz genießen Daten, die verwendet werden, um die Kreditwürdigkeit einer Person zu bewerten, oder solche, die die öffentliche Bekanntmachung von Verwaltungssanktionen betreffen. Siehe Artikel 21 Absatz 1 der Richtlinie 2014/17/EU des Europäischen Parlaments und des Rates vom 4. Februar 2014 über Wohnimmobilienkreditverträge für Verbraucher und zur Änderung der Richtlinien 2008/48/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie die Artikel 68 und 69 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG. Ein weiteres Beispiel findet sich in den Vorschriften zu klinischen Prüfungen, siehe die Artikel 28 bis 35 der Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG.

Sicherheitszwecken). Infolgedessen sind die Datenschutzbehörden in vollem Umfang für die Beurteilung der Rechtmäßigkeit aller anderen Verarbeitungsvorgänge zuständig, die auf die Speicherung von oder den Zugriff auf Informationen auf dem Gerät des Endnutzers folgen.[42]

76. Ein Verstoß gegen die DSGVO kann auch ein Verstoß gegen nationale e-Datenschutz-Vorschriften sein. Die Datenschutzbehörde kann einen festgestellten Verstoß gegen e-Datenschutz-Vorschriften bei der Anwendung der DSGVO berücksichtigen (z. B. bei der Beurteilung der Einhaltung des Grundsatzes von Rechtmäßigkeit und Treu und Glauben nach Artikel 5 Absatz 1 Buchstabe a der DSGVO). Gleichwohl muss jede Entscheidung zur Durchsetzung auf Grundlage der DSGVO begründet werden, es sei denn, der Datenschutzbehörde wurden durch das Recht des Mitgliedstaates zusätzliche Zuständigkeiten übertragen.

77. Wenn eine Datenschutzbehörde nach nationalem Recht als zuständige Behörde nach der e-Datenschutz-Richtlinie eingesetzt wurde, besitzt sie die Zuständigkeit, nationale e-Datenschutz-Vorschriften unmittelbar und zusätzlich zur DSGVO durchzusetzen (andernfalls besitzt sie diese Zuständigkeit nicht).

78. Allgemein gilt es in Fällen, in denen mehrere Behörden für die unterschiedlichen Rechtsvorschriften zuständig sind, sicherzustellen, dass die Durchsetzung beider Rechtsvorschriften auf kohärente Weise erfolgt, um insbesondere bei im Zusammenhang mit Verarbeitungsvorgängen erfolgten, eng miteinander verbunden Verstößen gegen Bestimmungen der DSGVO und der e-Datenschutz-Richtlinie eine Verletzung des Verbots der doppelten strafrechtlichen Belangung („ne bis in idem“) zu vermeiden.

6 ANWENDBARKEIT DES VERFAHRENS DER ZUSAMMENARBEIT UND DES KOHÄRENZVERFAHRENS

79. Die dritte Frage der belgischen Datenschutzbehörde an den Ausschuss kann folgendermaßen umschrieben werden:

[42] In dieser Hinsicht sollte auf die Stellungnahmen der Artikel-29-Datenschutzgruppe zum berechtigten Interesse (06/2014) und zur Zweckbindung („Opinion 03/2013 on purpose limitation“; nur Englisch) Bezug genommen werden, in denen klargestellt wird, dass bestimmte Formen der Werbung auf Basis von Behavioural Targeting nicht nur aufgrund von Artikel 5 Absatz 3 der Zustimmung der betroffenen Person bedürfen. Hierzu heißt es in der Stellungnahme zur Zweckbindung, dass als zweites Szenario denkbar ist, dass eine Organisation eigens die persönlichen Vorlieben, das Verhalten oder die Einstellungen individueller Kunden analysieren oder vorhersagen möchte und die diesbezüglichen Ergebnisse in der Folge als Grundlage für Maßnahmen oder Entscheidungen herangezogen werden, die in Bezug auf diese Kunden getroffen werden. In diesen Fällen sei somit eine freie, spezifische, informierte und eindeutige Einwilligung fast immer erforderlich, andernfalls könne die weitere Verwendung nicht mehr als konform gelten. Besonders wichtig sei daher das Erfordernis einer solchen Einwilligung zum Beispiel beim Tracking oder Profiling zu Zwecken des Direktmarketings, der Werbung auf Basis von Behavioural Targeting, der Datenvermittlung, der standortbasierten Werbung oder der trackingbasierten digitalen Marktforschung.
In der Stellungnahme zum berechtigten Interesse heißt es hierzu:
„Anstatt lediglich die Möglichkeit anzubieten, diese Art von Profiling und gezielter Werbung zu verweigern, wäre eine Einwilligung in Kenntnis der Sachlage nach Artikel 7 Buchstabe a sowie nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation erforderlich. Daher sollte Artikel 7 Buchstabe f nicht als Rechtsgrundlage für die Verarbeitung herangezogen werden.“

- *In welchem Umfang sind das Verfahren der Zusammenarbeit und das Kohärenzverfahren auf eine Verarbeitung anwendbar, die - zumindest in Bezug auf bestimmte Verarbeitungsvorgänge - in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt?*

80. In Anlehnung an Kapitel VII der DSGVO betreffen das Verfahren der Zusammenarbeit und das Kohärenzverfahren, die den Datenschutzbehörden gemäß der DSGVO zur Verfügung stehen, die Überwachung der Anwendung der Bestimmungen der DSGVO. Die in der DSGVO vorgesehenen Verfahren gelten nicht für die Durchsetzung der in der e-Datenschutz-Richtlinie enthaltenen Bestimmungen als solcher.

81. In jedem Fall ist in Artikel 15 Absatz 3 der e-Datenschutz-Richtlinie Folgendes vorgesehen:

> *„[Der Europäische Datenschutzausschuss] nimmt auch die in [Artikel 70 der Verordnung (EU) 2016/679] festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr.“*

82. Was die Zusammenarbeit zwischen den für die Durchsetzung der e-Datenschutz-Richtlinie zuständigen Behörden anbetrifft, bestimmt Artikel 15a Absatz 4 der e-Datenschutz-Richtlinie Folgendes: *„Zur Gewährleistung einer wirksamen grenzübergreifenden Koordinierung der Durchsetzung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften und zur Schaffung harmonisierter Bedingungen für die Erbringung von Diensten, mit denen ein grenzüberschreitender Datenfluss verbunden ist, können die zuständigen nationalen Regulierungsbehörden Maßnahmen erlassen*.“

83. Diese grenzübergreifende Zusammenarbeit zwischen Behörden, die für die Durchsetzung der e-Datenschutz-Richtlinie zuständig sind (einschließlich Datenschutzbehörden, nationale Regulierungsbehörden und andere Behörden), kann in dem Maße erfolgen, wie die betreffenden nationalen Regulierungsbehörden Maßnahmen erlassen, die eine solche Zusammenarbeit ermöglichen.

84. Diesbezüglich ist anzumerken, dass das Verfahren der Zusammenarbeit und das Kohärenzverfahren gleichwohl in vollem Umfang anzuwenden sind, wenn die Verarbeitung den allgemeinen Bestimmungen der DSGVO unterliegt (und nicht einer in der e-Datenschutz-Richtlinie enthaltenen „speziellen Bestimmung“). Auch wenn beispielsweise die Verarbeitung personenbezogener Daten (z. B. zur Profilerstellung) zum Teil auf dem Zugriff auf Informationen beruht, die im Gerät des Endnutzers gespeichert sind, müssen die Datenschutzvorschriften, die nicht in der e-Datenschutz-Richtlinie vorgesehen sind (z. B. Rechte betroffener Personen, Verarbeitungsprinzipien), für die Verarbeitung personenbezogener Daten, die nach dem Zugriff auf die im Gerät des Endnutzers gespeicherten Informationen erfolgt, den Bestimmungen der DSGVO einschließlich des Verfahrens der Zusammenarbeit und des Kohärenzverfahrens unterliegen.

85. In der Praxis werden die Datenschutzbehörden den zu nutzenden „Übermittlungsweg“ sorgfältig wählen müssen, insbesondere, wenn sie nicht nur die DSGVO durchzusetzen haben, sondern auch für die Durchsetzung (eines Teils) der nationalen Umsetzung der e-Datenschutz-Richtlinie zuständig sind. Der - in Kapitel VII (Zusammenarbeit und Kohärenz) der DSGVO beschriebene - Standard-„Übermittlungsweg“ muss für jeden einzelnen Teil des Verfahrens genutzt werden, das den Einsatz der durch die DSGVO verliehenen Durchsetzungsbefugnisse in Reaktion auf einen Verstoß gegen die

DSGVO vorsieht. Der im Ermessen liegende „Übermittlungsweg“ kann von Datenschutzbehörden im Zusammenhang mit den spezifischen Durchsetzungsbefugnissen verwendet werden, die ihnen durch die nationale Umsetzung der e-Datenschutz-Richtlinie verliehen wurden, falls das betreffende Verfahren darauf abzielt, Verstöße gegen nationale e-Datenschutz-Vorschriften zu ahnden, welche durch die e-Datenschutz-Richtlinie geregelte spezifische Handlungen betreffen. Sobald Fragen betroffen sind, die in den Anwendungsbereich der DSGVO fallen, sind die Datenschutzbehörden verpflichtet, das in der DSGVO vorgesehene Verfahren der Zusammenarbeit und das Kohärenzverfahren anzuwenden.

7 ZUSAMMENFASSUNG

- *Schränkt allein schon die Tatsache, dass die Verarbeitung personenbezogener Daten in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt, die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden nach der DSGVO ein? Gibt es mit anderen Worten einen Teilsatz von Datenverarbeitungsvorgängen, den sie nicht berücksichtigen müssen, und wenn ja, in welchen Fällen?*

86. Wenn die Verarbeitung personenbezogener Daten in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt, haben die Datenschutzbehörden nur dann die Zuständigkeit, die durch nationale e-Datenschutz-Vorschriften geregelten Datenverarbeitungsvorgänge zu untersuchen, wenn das nationale Gesetz ihnen diese Zuständigkeit überträgt, und diese Untersuchung muss innerhalb der Grenzen der Aufsichtsbefugnisse erfolgen, die der Behörde durch das nationale Recht zur Umsetzung der e-Datenschutz-Richtlinie übertragen wurden.

87. Die Datenschutzbehörden sind für die Durchsetzung der DSGVO zuständig. Die bloße Tatsache, dass ein Teilsatz der Verarbeitung in den Anwendungsbereich der e-Datenschutz-Richtlinie fällt, schränkt die Zuständigkeit von Datenschutzbehörden nach der DSGVO nicht ein.

- *Müssen Datenschutzbehörden bei der Ausübung ihrer in der DSGVO festgelegten Zuständigkeiten, Aufgaben und Befugnisse die Bestimmungen der e-Datenschutz-Richtlinie berücksichtigen, und wenn ja, inwieweit? Anders ausgedrückt: Sollten Verstöße gegen nationale e-Datenschutz-Vorschriften bei der Beurteilung der Einhaltung der DSGVO berücksichtigt oder außer Acht gelassen werden, und wenn ja, unter welchen Umständen??*

88. Die Behörde oder die Behörden, denen die Zuständigkeit durch die Mitgliedstaaten im Sinne der e-Datenschutz-Richtlinie verliehen wurde, sind ausschließlich für die Durchsetzung jener nationalen Bestimmungen zur Umsetzung der e-Datenschutz-Richtlinie verantwortlich, die den spezifischen Verarbeitungsvorgang betreffen; dies schließt auch solche Fälle ein, in denen die Verarbeitung personenbezogener Daten in den Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt. Gleichwohl sind die Datenschutzbehörden weiter in vollem Umfang für alle Verarbeitungen von personenbezogenen Daten zuständig, die nicht unter eine oder mehrere spezifische Bestimmungen der e-Datenschutz-Richtlinie fallen.

89. Ein Verstoß gegen die DSGVO kann auch ein Verstoß gegen nationale e-Datenschutz-Vorschriften sein. Die Datenschutzbehörde kann einen festgestellten Verstoß gegen e-Datenschutz-Vorschriften

bei der Anwendung der DSGVO berücksichtigen (z. B. bei der Beurteilung der Einhaltung des Grundsatzes von Rechtmäßigkeit und Treu und Glauben nach Artikel 5 Absatz 1 Buchstabe a der DSGVO). Gleichwohl muss jede Entscheidung zur Durchsetzung auf Grundlage der DSGVO begründet werden, es sei denn, der Datenschutzbehörde wurden durch das Recht des Mitgliedstaates zusätzliche Zuständigkeiten übertragen.

90. Wenn eine Datenschutzbehörde nach nationalem Recht als zuständige Behörde nach der e-Datenschutz-Richtlinie eingesetzt wurde, besitzt sie die Zuständigkeit, nationale e-Datenschutz-Vorschriften unmittelbar und zusätzlich zur DSGVO durchzusetzen (andernfalls besitzt sie diese Zuständigkeit nicht).

- *In welchem Umfang sind das Verfahren der Zusammenarbeit und das Kohärenzverfahren auf eine Verarbeitung anwendbar, die - zumindest in Bezug auf bestimmte Verarbeitungsvorgänge - in den sachlichen Anwendungsbereich sowohl der DSGVO als auch der e-Datenschutz-Richtlinie fällt?*

91. Das Verfahren der Zusammenarbeit und das Kohärenzverfahren, die den Datenschutzbehörden nach Kapitel VII der DSGVO zur Verfügung stehen, betreffen die Überwachung der Anwendung der Bestimmungen der DSGVO. Die in der DSGVO vorgesehenen Verfahren gelten nicht für die Durchsetzung der nationalen Anwendung der e-Datenschutz-Richtlinie. Das Verfahren der Zusammenarbeit und das Kohärenzverfahren sind gleichwohl in vollem Umfang anzuwenden, wenn die Verarbeitung den allgemeinen Bestimmungen der DSGVO unterliegt (und nicht einer in der e-Datenschutz-Richtlinie enthaltenen „speziellen Bestimmung“).

***

92. Der Ausschuss erkennt an, dass die vorstehende Auslegung das Ergebnis der laufenden Verhandlungen zur e-Datenschutz-Verordnung nicht berührt. Die vorgeschlagene Verordnung befasst sich mit vielen wichtigen Aspekten einschließlich der Zuständigkeiten von Datenschutzbehörden, aber auch mit anderen sehr wichtigen Fragen. Der Ausschuss wiederholt seinen Standpunkt, dass die Verabschiedung einer e-Datenschutz-Verordnung wichtig ist.[43]

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)

[43] Der Europäische Datenschutzausschuss hat die Europäische Kommission, das Parlament und den Rat ersucht, gemeinsam an einer raschen Verabschiedung der neuen e-Datenschutz-Verordnung zu arbeiten (Erklärung des Europäischen Datenschutzausschusses vom 25. Mai 2018).