Leitlinien 2/2023 zum technischen Anwendungsbereich von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation

Version 2.0

Angenommen am 7. Oktober 2024

Versionsverlauf

Version 1.0	14. November 2023	Annahme der Leitlinien zur öffentlichen Konsultation
Version 2.0	7. Oktober 2024	Annahme der Leitlinien nach öffentlicher Konsultation

Zusammenfassung

In diesen Leitlinien befasst sich der EDPB mit der Anwendbarkeit von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation auf verschiedene technische Lösungen. Diese Leitlinien bauen auf die Stellungnahme 9/2014 der Artikel-29-Datenschutzgruppe zur Anwendung der Datenschutzrichtlinie für elektronische Kommunikation auf die Nutzung des virtuellen Fingerabdrucks auf und sollen ein klares Verständnis der technischen Vorgänge vermitteln, die unter Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation fallen.

Das Aufkommen neuer Tracking-Methoden, die sowohl bestehende Tracking-Instrumente ersetzen (z. B. Cookies, da einige Browserhersteller die Unterstützung für Cookies von Drittanbietern eingestellt haben) als auch neue Geschäftsmodelle schaffen, wirft schwierige Fragen zum Datenschutz auf. Während die Anwendbarkeit von Artikel 5 Absatz 3 der Richtlinie für elektronische Kommunikation für einige Tracking-Technologien wie Cookies gut etabliert und umgesetzt ist, müssen Unklarheiten im Zusammenhang mit der Anwendung der genannten Bestimmung auf neue Trackinginstrumente ausgeräumt werden.

Die Leitlinien benennen drei Schlüsselelemente für die Anwendbarkeit von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation (Abschnitt 2.1), nämlich „Informationen“, „Endgerät eines Teilnehmers oder Nutzers“ und „Zugriff“, „Speicherung von Informationen“ sowie „gespeicherte Informationen“. Die Leitlinien enthalten ferner eine detaillierte Analyse der einzelnen Elemente (Abschnitte 2.2 bis 2.6).

In Abschnitt 3 wird diese Analyse auf eine nicht erschöpfende Liste von Anwendungsfällen angewandt, die verbreitete Techniken darstellen:

- URL- und Pixel-Tracking
- Lokale Verarbeitung
- Tracking nur auf der Grundlage der IP-Adresse
- Intermittierende und vermittelte Meldung über das Internet der Dinge (Internet of Things, IoT)
- Eindeutige Kennungen

Inhalt

1 Einleitung 5

2 Analyse 6

2.1 Schlüsselelemente für die Anwendbarkeit von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation 6

2.2 Begriff der „Information“ – Kriterium A 7

2.3 Begriff des „Endgeräts eines Teilnehmers oder Nutzers“ – Kriterium B.1 7

2.4 Begriff des „öffentlichen Kommunikationsnetzes“ – Kriterium B.2 9

2.5 Begriff „Zugriff“ – Kriterium C.1 10

2.6 Begriffe der „Speicherung von Informationen“ und „gespeicherte Informationen“ – Kriterium C.2 12

3 Anwendungsfälle 12

3.1 URL- und Pixel-Tracking 14

3.2 Lokale Verarbeitung 15

3.3 Tracking nur auf der Grundlage der IP-Adresse 15

3.4 Intermittierende und vermittelte Meldung über das Internet der Dinge 15

3.5 Eindeutige Kennungen 16

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 70 Absatz 1 Buchstabe e 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, insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung[1],

gestützt auf Artikel 15 Absatz 3 der 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, geändert durch die Richtlinie 2009/136/EG (im Folgenden „ePrivacy-RL“),

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung –

HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN:

1 EINLEITUNG

1. Gemäß Artikel 5 Absatz 3 ePrivacy-RL ist *„die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind“*, nur auf Grundlage einer Einwilligung oder im Falle einer Erforderlichkeit für bestimmte in diesem Artikel genannte Zwecke gestattet. Wie Erwägungsgrund 24 ePrivacy-RL[2] in Erinnerung ruft, besteht das Ziel dieser Bestimmung darin, die Endgeräte der Nutzer zu schützen, da sie Teil der Privatsphäre der Nutzer sind. Aus dem Wortlaut des Artikels ergibt sich, dass Artikel 5 Absatz 3 ePrivacy-RL nicht ausschließlich für Cookies, sondern auch für „ähnliche Technologien“ gilt. Allerdings gibt es derzeit keine umfassende Liste der technischen Vorgänge, die unter Artikel 5 Absatz 3 ePrivacy-RL fallen.

2. Die Artikel 29-Datenschutzgruppe (im Folgenden „WP29“) hat in ihrer Stellungnahme 9/2014 zur Anwendung der Datenschutzrichtlinie für elektronische Kommunikation auf die Nutzung des virtuellen Fingerabdrucks (im Folgenden „WP29-Stellungnahme 9/2014“) bereits klargestellt, dass die Nutzung des virtuellen Fingerabdrucks in den technischen Anwendungsbereich von Artikel 5 Absatz 3 der ePrivacy-RL fällt[3], aufgrund der neuen technologischen Fortschritte sind jedoch weitere Leitlinien in Bezug auf die derzeit angewandten Tracking-Techniken erforderlich. Die technische Landschaft hat sich in den letzten zehn Jahren durch die zunehmende Verwendung von in Betriebssysteme

[1] Soweit in dieser Stellungnahme auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

[2] „Die Endgeräte von Nutzern elektronischer Kommunikationsnetze und in diesen Geräten gespeicherte Informationen sind Teil der Privatsphäre der Nutzer, die dem Schutz aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt. So genannte „Spyware“, „Web-Bugs“, „Hidden Identifiers“ und ähnliche Instrumente können ohne das Wissen des Nutzers in dessen Endgerät eindringen, um Zugriff auf Informationen zu erlangen, um versteckte Informationen dort abzulegen oder die Nutzeraktivität zu verfolgen und können eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen. Die Verwendung solcher Instrumente sollte nur für rechtmäßige Zwecke mit dem Wissen der betreffenden Nutzer gestattet sein.“

[3] WP29-Stellungnahme 9/2014, S. 12.

eingebetteten Kennungen sowie durch die Schaffung neuer Instrumente, die die Speicherung von Informationen in Endgeräten ermöglichen, weiterentwickelt.

3. Die Unklarheiten bezüglich des Anwendungsbereichs von Artikel 5 Absatz 3 ePrivacy- haben Anreize für den Einsatz alternativer Lösungen zum Tracken von Internetnutzern geschaffen und fördern die Tendenz, die in Artikel 5 Absatz 3 ePrivacy-RL vorgesehenen rechtlichen Verpflichtungen zu umgehen. Alle diese Fälle geben Anlass zu Bedenken und erfordern eine ergänzende Analyse, um die vorherigen Leitlinien des EDSA zu ergänzen.

4. Ziel dieser Leitlinien ist es, eine technische Analyse des Anwendungsbereichs von Artikel 5 Absatz 3 ePrivacy-RL vorzunehmen, d. h. zu klären, was technisch unter die Formulierung „*Informationen zu speichern oder Zugriff auf Informationen zu erhalten, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind*“ fällt. Diese Leitlinien gehen nicht auf die Umstände ein, unter denen eine Verarbeitung unter die in der Datenschutzrichtlinie für elektronische Kommunikation[4] vorgesehenen Ausnahmen vom Erfordernis der Einwilligung fallen kann, da diese Umstände von Fall zu Fall unter Berücksichtigung der einschlägigen Umsetzungsvorschriften der Mitgliedstaaten und der von den zuständigen nationalen Behörden herausgegebenen Leitlinien geprüft werden sollten.

5. Eine nicht erschöpfende Liste spezifischer Anwendungsfälle wird im letzten Teil dieser Leitlinien analysiert.

2 ANALYSE

2.1 Schlüsselelemente für die Anwendbarkeit von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation

6. Artikel 5 Absatz 3 ePrivacy-RL findet Anwendung, wenn:

   a. **KRITERIUM A:** die durchgeführten Vorgänge sich auf „*Informationen*“ beziehen. Es sei darauf hingewiesen, dass es sich bei dem verwendeten Begriff nicht um „personenbezogene Daten“, sondern um „Informationen“ handelt.

   b. **KRITERIUM B:** die durchgeführten Vorgänge ein „*Endgerät*“ eines Teilnehmers oder Nutzers (B.1) betreffen, was die Notwendigkeit impliziert, den Begriff *eines „öffentlichen Kommunikationsnetzes*“ (B.2) zu bewerten.

   c. **KRITERIUM C** es sich bei den durchgeführten Vorgängen tatsächlich um eine „*Speicherung*“ (C.1) oder einen „*Zugriff*“ (C.2) handelt. Diese beiden Begriffe können unabhängig voneinander untersucht werden, wie in der WP29-Stellungnahme 9/2014 angemerkt wurde: *„Die Verwendung der Begriffe „gespeichert oder abgerufen“ deutet darauf hin, dass die Speicherung und der Zugriff nicht im Rahmen derselben Kommunikation erfolgen und nicht von derselben Partei vorgenommen werden müssen“*[5].

[4] In Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation heißt es: „*Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige 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.*“

[5] WP29-Stellungnahme 9/2014, S. 9.

Aus Gründen der Lesbarkeit wird die Stelle, welche auf die im Endgerät des Nutzers gespeicherten Informationen zugreift, im Folgenden als „zugreifende Stelle“ bezeichnet.

2.2 Begriff der „Information“ – Kriterium A

7. Wie in KRITERIUM A dargelegt, wird in diesem Abschnitt erläutert, was unter den Begriff „Informationen“ fällt. Die Wahl des Begriffs „Informationen“, welcher weiter als der enge Begriff der personenbezogenen Daten gefasst ist, steht im Zusammenhang mit dem Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation.

8. Ziel von Artikel 5 Absatz 3 ePrivacy-RL ist es, die Privatsphäre der Nutzer zu schützen, wie es in Erwägungsgrund 24 heißt: „*Die Endgeräte von Nutzern elektronischer Kommunikationsnetze und in diesen Geräten gespeicherte Informationen sind Teil der Privatsphäre der Nutzer, die dem Schutz aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt.*“ Sie ist auch durch Artikel 7 der Charta der Grundrechte der Europäischen Union geschützt.

9. Tatsächlich fallen Szenarien, die in diesen privaten Bereich eingreifen, ausdrücklich unter den Wortlaut von Artikel 5 Absatz 3 und Erwägungsgrund 24 ePrivacy-RL, selbst wenn keine personenbezogener Daten betroffen sind, so z. B. die Speicherung von Viren auf dem Endgerät des Nutzers. Dies zeigt, dass die Definition des Begriffs „Informationen“ nicht einschränkend dahingehend verstanden werden sollte, sich auf eine identifizierte oder identifizierbare natürliche Person zu beziehen.

10. Dies wurde vom Gerichtshof der Europäischen Union bestätigt: „Dieser Schutz erstreckt sich auf alle in solchen Endgeräten gespeicherten Informationen, unabhängig davon, ob es sich um personenbezogene Daten handelt, und erfasst insbesondere – wie ebenfalls aus diesem Erwägungsgrund hervorgeht – „Hidden Identifiers“ oder ähnliche Instrumente, die ohne das Wissen der Nutzer in deren Endgeräte eindringen.“[6].

11. Die Fragen, ob die Herkunft dieser Informationen und die Gründe, warum sie im Endgerät gespeichert werden, bei der Beurteilung der Anwendbarkeit von Artikel 5 Absatz 3 ePrivacy-RL berücksichtigt werden sollten, wurden bereits geklärt. Zum Beispiel in der Stellungnahme der WP29 9/2014: „*Dies darf nicht dahingehend ausgelegt werden, dass der Dritte die Einwilligung zum Zugriff auf diese Informationen nicht braucht, nur weil er sie nicht gespeichert hat. Das Einwilligungserfordernis besteht auch für einen Lesezugriff auf einen Festwert (beispielsweise für die Abfrage der MAC-Adresse einer Netzschnittstelle über die OS-API).*“[7].

12. Zusammenfassend lässt sich sagen, dass der Begriff „Informationen“ sowohl nicht personenbezogene Daten als auch personenbezogene Daten umfasst, unabhängig davon, wie und von wem diese Daten gespeichert wurden, d. h. ob von einer externen Stelle (einschließlich anderer Stellen als derjenigen, die Zugang haben), vom Nutzer, von einem Hersteller oder einem anderen Szenario.

2.3 Begriff des „Endgeräts eines Teilnehmers oder Nutzers“ – Kriterium B.1

13. Dieser Abschnitt stützt sich auf die Begriffsbestimmung, die in der Richtlinie 2008/63/EG verwendet wird und auf die in Artikel 2 der Richtlinie (EU) 2018/1972 Bezug genommen wird, wobei „Endgeräte“ definiert sind als: „*direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtungen zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden; bei einem*

[6]Urteil des Gerichtshofs vom 1. Oktober 2019, Planet 49, Rechtssache C-673/17, ECLI:EU:C:2019:801, Rn. 70.
[7] WP29-Stellungnahme 9/2014, S. 9.

indirekten Anschluss ist zwischen der Endeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet“[8].

14. Erwägungsgrund 24 ePrivacy-RL vermittelt ein klares Verständnis der Rolle der Endgeräte für den durch Artikel 5 Absatz 3 ePrivacy-RL gebotenen Schutz. Die Datenschutzrichtlinie für elektronische Kommunikation schützt die Privatsphäre der Nutzer nicht nur in Bezug auf die Vertraulichkeit ihrer Informationen, sondern auch durch die Wahrung der Integrität der Endgeräte des Nutzers. Dieses Verständnis wird bei der Auslegung des Begriffs „Endgerät“ in diesen Leitlinien zugrunde gelegt.

15. Nach Artikel 3 ePrivacy-RL muss die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen erfolgen, damit die Datenschutzrichtlinie für elektronische Kommunikation Anwendung findet. Dies bedeutet, dass ein Gerät in Verbindung mit einem solchen Dienst nutzbar sein sollte und dass es, um Endgerät zu sein, an die Schnittstelle eines öffentlichen Kommunikationsnetzes angeschlossen oder anschließbar[9] sein sollte. Der EDSA stellt fest, dass durch die 2009 vorgenommenen Änderungen[10] des Wortlauts von Artikel 5 Absatz 3 ePrivacy-RL der Schutz der Endgeräte ausgeweitet wurde, indem der Verweis auf die „Benutzung elektronischer Kommunikationsnetze“ als Mittel zur Speicherung von Informationen oder zum Zugriff auf Informationen, die im Endgerät gespeichert sind, gestrichen wurde. Daher gilt Artikel 5 Absatz 3 ePrivacy-RL, solange ein Gerät über eine Netzschnittstelle verfügt, über die eine Verbindung erfolgen kann (auch wenn eine solche Verbindung nicht besteht), für jede Stelle, die Informationen auf dem Endgerät speichert und auf bereits im Endgerät gespeicherte Informationen zugreift, unabhängig davon, auf welche Weise der Zugriff auf das Endgerät erfolgt und ob es angeschlossen oder von einem Netz getrennt ist.

16. Geräte, die Teil des öffentlichen elektronischen Kommunikationsnetzes selbst sind, sind nicht als Endgerät im Sinne von Artikel 5 Absatz 3 ePrivacy-RL zu betrachten.[11]

17. Ein Endgerät kann aus einer beliebigen Anzahl einzelner Hardwareteile bestehen, die zusammen das Endgerät bilden. Dabei kann, muss es sich aber nicht, um ein physisch geschlossenes Gerät handeln, in dem die gesamte Anzeige-, Verarbeitungs-, Speicher- und Peripheriehardware enthalten ist (z. B. Smartphones, Laptops, netzgebundene Speichergeräte, vernetzte Autos oder vernetzte Fernsehgeräte, Smartglasses).

18. Die Datenschutzrichtlinie für elektronische Kommunikation erkennt an, dass der Schutz der Vertraulichkeit der auf dem Endgerät des Nutzers gespeicherten Informationen und der Integrität des Endgeräts des Nutzers nicht auf den Schutz der Privatsphäre natürlicher Personen beschränkt ist, sondern auch das Recht auf Achtung ihrer Kommunikationsfreiheit oder die berechtigten Interessen

[8] Richtlinie 2008/63/EG der Kommission vom 20. Juni 2008 über den Wettbewerb auf dem Markt für Telekommunikationsendeinrichtungen (ABl. L 162 vom 21.6.2008, S. 20).

[9] Das heißt, es muss über die technischen Möglichkeiten verfügen, an das Netz angeschlossen zu werden, auch wenn diese Verbindung derzeit nicht vorhanden ist.

[10] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (Text von Bedeutung für den EWR) (ABl. L 337 vom 18.12.2009, S. 11).

[11] Zur Ermittlung der Grenzen des Netzes in verschiedenen Zusammenhängen siehe die GEREK-Leitlinien für gemeinsame Herangehensweisen zur Bestimmung des Netzterminierungspunkts in verschiedenen Netztopologien (BoR (20) 46).

juristischer Personen betrifft[12]. Ein Endgerät, das der Kommunikation und den berechtigten Interessen juristischer Personen dient, ist daher durch Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation geschützt.

19. Der Nutzer oder Teilnehmer kann Eigentümer des Endgeräts sein, es mieten oder auf andere Weise mit ihm ausgestattet sein. Mehrere Nutzer oder Teilnehmer können dasselbe Endgerät gemeinsam nutzen.

20. Dieser durch die Datenschutzrichtlinie für elektronische Kommunikation gewährte Schutz wird für die dem Nutzer oder Teilnehmer zuzuordnenden Endgeräte gewährleistet und ist nicht davon abhängig, ob der Nutzer die Zugriffswege eingerichtet hat (z. B. ob er die elektronische Kommunikation eingeleitet hat) oder ob der Nutzer sich der genannten Zugriffswege bewusst ist.

2.4 Begriff des „öffentlichen Kommunikationsnetzes" – Kriterium B.2

21. Da es sich bei der in der Datenschutzrichtlinie für elektronische Kommunikation geregelten Situation um die *„Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft"*[13] handelt und die Definition eines Endgeräts ausdrücklich den Begriff *„öffentliches Kommunikationsnetz"* erwähnt, ist es von entscheidender Bedeutung, diesen Begriff zu klären, um den Kontext zu bestimmen, in dem Artikel 5 Absatz 3 ePrivacy-RL Anwendung findet.

22. Der Begriff des elektronischen Kommunikationsnetzes ist in der Datenschutzrichtlinie für elektronische Kommunikation selbst nicht definiert. Auf dieses Konzept wurde ursprünglich in der Richtlinie 2002/21/EG (Rahmenrichtlinie) über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste[14] Bezug genommen, die später durch Artikel 2 Absatz 1 der Richtlinie 2018/1972 (Europäischer Kodex für elektronische Kommunikation) ersetzt wurde. Der Text lautet nunmehr:

> *„elektronisches Kommunikationsnetz": Übertragungssysteme, ungeachtet dessen, ob sie auf einer permanenten Infrastruktur oder zentralen Verwaltungskapazität basieren, und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen – einschließlich der nicht aktiven Netzbestandteile –, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelt, einschließlich Internet) und mobile Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hör- und Fernsehfunk sowie Kabelfernsehnetze, unabhängig von der Art der übertragenen Informationen.*[15]

23. Diese Definition ist in Bezug auf die Übertragungstechnologien neutral. Ein elektronisches Kommunikationsnetz im Sinne dieser Definition ist jedes Netzwerksystem, das die Übertragung

[12] In der Tat kann der Nutzer eine natürliche oder eine juristische Person sein, wie sich aus Artikel 2 Absatz 13 der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation ergibt.

[13] Artikel 3 ePrivacy-RL.

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

→ Kommentar: Handelt es sich hier vielleicht um eine neue Fußnote

[15] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) (Text von Bedeutung für den EWR), Artikel 2 Absatz 1.

elektronischer Signale zwischen seinen Knotenpunkten ermöglicht, unabhängig von den verwendeten Geräten und Protokollen.

24. Der Begriff des elektronischen Kommunikationsnetzes im Sinne der Richtlinie (EU) 2018/1972 hängt weder vom öffentlichen oder privaten Charakter der Infrastruktur noch von der Art und Weise ab, wie das Netz aufgebaut oder verwaltet wird („*ungeachtet dessen, ob sie auf einer permanenten Infrastruktur oder zentralen Verwaltungskapazität basieren*“[16]). Folglich ist die Definition des Begriffs „elektronisches Kommunikationsnetz“ gemäß Artikel 2 der Richtlinie (EU) 2018/1972 so weit gefasst, dass sie jede Art von Infrastruktur umfasst. Dazu gehören Netze, unabhängig davon, ob sie von einem Betreiber verwaltet werden oder nicht, Netze, die von einer Gruppe von Betreibern gemeinsam verwaltet werden, oder sogar Ad-hoc-Netze, in denen sich ein Endgerät unter Verwendung von Kurzstrecken-Übertragungsprotokollen dynamisch einem Netz anderer Endgeräte anschließen oder es verlassen kann.

25. Diese Definition des Begriffs „Netzwerk“ enthält keinerlei Beschränkung in Bezug auf die Anzahl der Endgeräte, die sich zu irgendeinem Zeitpunkt im Netzwerk befinden. Einige Vernetzungssysteme beruhen darauf, dass Knotenpunkte Informationen ad hoc an aktuell verbundene Knotenpunkte weiterleiten[17] und über die zeitweise auch nur zwei Teilnehmer miteinander kommunizieren können. Solche Fälle können in den allgemeinen Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation fallen, solange das Netzprotokoll eine weitere Einbeziehung von Peers ermöglicht.

26. Die öffentliche Verfügbarkeit des Kommunikationsnetzes ist für die Einstufung des Geräts als Endgerät und damit für die Anwendbarkeit von Artikel 5 Absatz 3 ePrivacy-RL erforderlich. Es sei darauf hingewiesen, dass die Tatsache, dass das Netz einem begrenzten Teil der Öffentlichkeit zur Verfügung gestellt wird (z. B. Abonnenten, ob zahlend oder nicht, die Zugangsvoraussetzungen unterliegen), ein solches Netz nicht zu einem privaten Netz macht[18].

2.5 Begriff „Zugriff“ – Kriterium C.1

27. Um den Begriff des „Zugriffs“ korrekt zu definieren, ist es wichtig, den Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation zu berücksichtigen, der in Artikel 1 festgelegt ist: „*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*“.

28. Kurz gesagt handelt es sich bei der Datenschutzrichtlinie für elektronische Kommunikation um ein Rechtsinstrument zum Schutz der Privatsphäre, das die Vertraulichkeit der Kommunikation und die Integrität von Geräten schützen soll. In Erwägungsgrund 24 ePrivacy-RL wird klargestellt, dass im Falle natürlicher Personen das Endgerät des Nutzers Teil seiner Privatsphäre ist und dass der Zugriff auf die

[16] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) (Text von Bedeutung für den EWR), Artikel 2 Absatz 1.

[17] Zum Beispiel im Zusammenhang mit verzögerungstoleranten Netzwerken, die „Store-and-Forward-Techniken“ wie das Open-Source-Projekt Briar verwenden.

[18] Für weitere Analysen zur Identifizierung öffentlicher Kommunikationsnetze wird auf die GEREK-Leitlinien zur Umsetzung der Verordnung über ein offenes Internet (BoR (20) 112) verwiesen. [Anm.: Leitlinien wurden überarbeitet, letzte Fassung vom 09.06.2022, BoR (22) 81].

darauf gespeicherten Informationen ohne sein Wissen eine ernsthafte Verletzung seiner Privatsphäre darstellen kann.

29. Auch juristische Personen werden durch die Datenschutzrichtlinie für elektronische Kommunikation geschützt[19]. Folglich ist der Begriff „Zugriff" im Sinne von Artikel 5 Absatz 3 ePrivacy-RL so auszulegen, dass diese Rechte vor Verletzungen durch Dritte geschützt werden.

30. Die Speicherung von Informationen oder der Zugriff darauf können unabhängige Vorgänge sein, die von unabhängigen Stellen durchgeführt werden. Die Speicherung von Informationen und der Zugriff auf bereits gespeicherte Informationen müssen nicht beide vorliegen, damit Artikel 5 Absatz 3 ePrivacy-RL Anwendung findet.

31. Wie in der WP29-Stellungnahme 9/2014 festgestellt wird: „*Die Verwendung der Begriffe „gespeichert oder abgerufen" deutet darauf hin, dass die Speicherung und der Zugriff nicht im Rahmen derselben Kommunikation erfolgen und nicht von derselben Partei vorgenommen werden müssen. Informationen, die von einer Partei gespeichert wurden (darunter vom Nutzer oder Hersteller des Geräts gespeicherte Informationen) und später von einer anderen Partei abgerufen werden, fallen daher in den Anwendungsbereich von Artikel 5 Absatz 3.*"[20]. Folglich gibt es für die Anwendung des Begriffs „Zugriff" keine Beschränkungen in Bezug auf die Herkunft der Informationen auf dem Endgerät.

32. Wann immer eine Stelle Schritte unternimmt, um Zugriff auf im Endgerät gespeicherte Informationen zu erhalten, findet Artikel 5 Absatz 3 ePrivacy-RL Anwendung. In der Regel bedeutet dies, dass die zugreifende Stelle proaktiv bestimmte Anweisungen an das Endgerät sendet, um die gewünschten Informationen zurückzuerhalten. Dies ist beispielsweise bei Cookies der Fall, bei denen die zugreifende Stelle das Endgerät anweist, bei jedem nachfolgenden Aufruf des Hypertext Transfer Protocol („HTTP") proaktiv Informationen zu senden.

33. Dies ist auch der Fall, wenn die zugreifende Stelle Software auf dem Endgerät des Nutzers verbreitet, die gespeichert wird und dann proaktiv einen Endpunkt der Anwendungsprogrammierschnittstelle („API") über das Netz aufruft. Weitere Beispiele sind JavaScript-Codes, bei denen die zugreifende Stelle den Browser des Nutzers anweist, asynchrone Anfragen mit den gewünschten Informationen zu senden. Ein solcher Zugriff fällt eindeutig in den Anwendungsbereich von Artikel 5 Absatz 3 ePrivacy-RL, da die zugreifende Stelle das Endgerät ausdrücklich anweist, die Informationen zu übermitteln.

34. In einigen Fällen sind die Stelle, die das Endgerät anweist, die Zieldaten zurückzusenden, und die Stelle, die die Informationen empfängt, möglicherweise nicht identisch. Dies kann sich aus der Bereitstellung und/oder Nutzung eines gemeinsamen Mechanismus zwischen den beiden Stellen ergeben. Die Anweisung an das Gerät, bereits gespeicherte Informationen zu senden (z. B. durch die Verwendung eines Protokolls oder eines SDK[21], die das proaktive Senden von Informationen durch das Endgerät implizieren), ermöglicht ein Eindringen in das Endgerät, weshalb ein solcher Zugriff bedeutet, dass Artikel 5 Absatz 3 ePrivacy-RL Anwendung findet. Wie in der Stellungnahme der WP29 09/2014 festgestellt, kann dies der Fall sein, wenn eine Website das Endgerät durch die Einbindung eines Tracking-Pixels anweist, Informationen an Werbedienste Dritter zu senden[22]. Dieser Anwendungsfall wird in Abschnitt 3.1 näher erläutert.

[19] Erwägungsgrund 26 ePrivacy-RL, siehe Punkt 17 oben.
[20] WP29-Stellungnahme 9/2014, S. 9.
[21] Ein SDK („Software Development Kit") ist ein Bündel von Softwareentwicklungswerkzeugen, die zur Verfügung gestellt werden, um die Erstellung von Anwendungssoftware zu erleichtern.
[22] WP29-Stellungnahme 9/2014, S. 9.

2.6 Begriffe der „Speicherung von Informationen“ und „gespeicherte Informationen“ – Kriterium C.2

35. Die Speicherung von Informationen im Sinne von Artikel 5 Absatz 3 ePrivacy-RL bezieht sich auf die Speicherung von Informationen auf einem physischen elektronischen Speichermedium, das Teil des Endgeräts eines Nutzers oder Teilnehmers ist.[23]

36. In der Regel werden die Informationen im Endgerät eines Nutzers oder Teilnehmers nicht durch direkten Zugriff auf den Speicher des Geräts durch eine andere Partei gespeichert, sondern indem Software auf dem Endgerät angewiesen wird, bestimmte Informationen zu erzeugen. Die Speicherung, die über solche Anweisungen erfolgt, gilt als unmittelbar von der anderen Partei veranlasst. Dazu gehört auch die Nutzung etablierter Protokolle wie die Speicherung von Cookies im Browser sowie spezifischer Software, unabhängig davon, wer die Protokolle oder die Software auf dem Endgerät erstellt oder installiert hat.

37. Die Datenschutzrichtlinie für elektronische Kommunikation legt weder eine Ober- oder Untergrenze für die Zeit fest, die eine Information auf einem Speichermedium verbleiben muss, um als gespeichert zu gelten, noch gibt es eine Ober- oder Untergrenze für die Menge der zu speichernden Informationen.

38. Ebenso hängt der Begriff der Speicherung nicht von der Art des Mediums ab, auf dem die Informationen gespeichert werden. Typische Beispiele sind Festplattenlaufwerke („HDD“), Solid-State-Laufwerke („SSD“), elektrisch programmierbare und löschbare Festwertspeicher („EEPROM“) und Arbeitsspeicher („RAM“), aber auch weniger typische Szenarien, bei denen ein Medium wie ein Magnetband oder der Pufferspeicher (Cache) eines Prozessors („CPU“) involviert sind, sind nicht vom Anwendungsbereich ausgeschlossen. Das Speichermedium kann intern (z. B. über eine SATA-Verbindung) oder extern (z. B. über eine USB-Verbindung) angeschlossen werden.

39. Der Begriff „gespeicherte Informationen“ bezieht sich auf Informationen, die bereits auf dem Endgerät vorhanden sind, unabhängig von der Quelle oder der Art dieser Informationen. Dies beinhaltet alle Ergebnisse der Speicherung von Informationen im Sinne von Artikel 5 Absatz 3 ePrivacy-RL wie oben beschrieben (entweder durch dieselbe Partei, die später auf die Informationen zugreift, oder durch eine andere dritte Partei). Er umfasst ferner Ergebnisse von Informationsspeicherungsprozessen, die nicht in den Anwendungsbereich von Artikel 5 Absatz 3 ePrivacy-RL fallen, wie z. B. die Speicherung auf dem Endgerät durch den Nutzer oder Teilnehmer selbst oder durch einen Hardware-Hersteller (z. B. die MAC-Adressen von Netzwerkkarten), in das Endgerät integrierte Sensoren oder auf dem Endgerät ausgeführte Prozesse und Programme, die Informationen erzeugen können, welche von gespeicherten Informationen abhängen oder von ihnen abgeleitet sind, oder auch nicht.

3 ANWENDUNGSFÄLLE

40. Wie bereits in der Einleitung[24] erwähnt, analysieren diese Leitlinien nicht die Anwendung der Ausnahmen von der Verpflichtung zur Einholung der Einwilligung nach Artikel 5 Absatz 3 ePrivacy-RL. Der EDSA weist darauf hin, dass in allen Fällen, in denen Informationen gespeichert werden oder Zugriff auf bereits gespeicherte Informationen gewährt wird, geprüft werden muss, ob eine Einwilligung erforderlich ist oder ob eine Ausnahmeregelung nach Artikel 5

[23] Gemäß der Definition in Abschnitt 2.3 der vorliegenden Leitlinien.
[24] Siehe oben Punkt 3.

Absatz 3 ePrivacy-RL Anwendung finden könnte. Die Leser dieser Leitlinien sollten daher die Ausnahmeregelung nach Artikel 5 Absatz 3 ePrivacy-RL in ihrem konkreten Anwendungsfall im Lichte dieser technischen Analyse betrachten.

41. Unabhängig vom spezifischen Kontexts, in dem diese technischen Kategorien verwendet werden können, ist es möglich, ohne den Anspruch auf Vollständigkeit weitgefasste Kategorien von Kennungen und Informationen zu ermitteln, die regelmäßig verwendet werden und der Anwendbarkeit von Artikel 5 Absatz 3 ePrivacy-RL unterliegen können.

42. Die Netzwerkkommunikation beruht in der Regel auf einem mehrschichtigen Modell, das die Verwendung von Kennungen erfordert, um eine ordnungsgemäße Errichtung und Durchführung der Kommunikation zu ermöglichen. Die Übermittlung dieser Kennungen an entfernte Akteure erfolgt über Software nach vereinbarten Kommunikationsprotokollen. Wie oben dargelegt, steht die Tatsache, dass die empfangende Stelle möglicherweise nicht die Stelle ist, die die Übermittlung von Informationen anordnet, der Anwendung von Artikel 5 Absatz 3 ePrivacy-RL nicht entgegen. Dabei kann es sich um Routing von Kennungen wie der MAC- oder IP-Adresse des Endgeräts, aber auch um Sitzungskennungen (SSRC, Websocket-Kennungen) oder Authentifizierungs-Token handeln.

43. In gleicher Weise kann das Anwendungsprotokoll verschiedene Mechanismen zur Bereitstellung von Kontextdaten (wie HTTP-Header mit „Accept"-Feld oder dem User-Agent), Caching-Mechanismen (wie ETag[25]) oder andere Funktionen (wie Cookies oder HSTS[26]) enthalten. Auch hier kann die Nutzung dieser Mechanismen zur Erfassung von Informationen (z. B. im Zusammenhang mit der Erstellung eines virtuellen Fingerabdrucks[27] oder der Nachverfolgung von Ressourcen-Kennungen) bedeuten, dass Artikel 5 Absatz 3 ePrivacy-RL Anwendung findet.

44. Andererseits gibt es Kontexte, in denen lokale Anwendungen, die auf dem Endgerät installiert sind, bestimmte Informationen ausschließlich innerhalb des Endgeräts verwenden, wie dies bei System-APIs von Smartphones der Fall sein kann (Zugriff auf Kamera, Mikrofon, GPS-Sensor, Beschleunigerchip, Funkchip, lokaler Dateizugriff, Kontaktliste, Zugriff auf Kennungen usw.). Dies könnte auch bei Webbrowsern der Fall sein, die in dem Gerät gespeicherte oder erzeugte Informationen verarbeiten (z. B. Cookies, lokale Speicherung, WebSQL oder sogar Informationen, die von den Nutzern selbst bereitgestellt werden). Die Verwendung solcher Informationen durch eine Anwendung würde keinen „Zugriff auf bereits gespeicherte Informationen" im Sinne von Artikel 5 Absatz 3 ePrivacy-RL darstellen, solange die Informationen das Gerät nicht verlassen; wenn jedoch auf diese Informationen oder eine Ableitung dieser Informationen zugegriffen wird, würde Artikel 5 Absatz 3 ePrivacy-RL Anwendung finden.

45. Schließlich werden in manchen Fällen Schadsoftware-Elemente von Akteuren verbreitet, beispielsweise Crypto-Mining-Software oder Malware im allgemeinen, wobei die Verarbeitungsfähigkeiten der Endgeräte zugunsten des verbreitenden Akteurs genutzt werden. Die Verbreitung der genannten Schadsoftware in den Endgeräten der Nutzer würde eine „Speicherung" im Sinne von Artikel 5 Absatz 3 ePrivacy-RL darstellen. Sollte die Software darüber hinaus eine

[25] Die HTTP ETag ist eine Kennung, die es ermöglicht, bedingte Anfragen auf der Grundlage der Gültigkeit der im Cache gespeicherten Kundendaten zu stellen.

[26] Mit HTTP Strict Transport Security (HSTS) können Server festlegen, welche Ressourcen stets über HTTPS-Verbindungen angefordert werden sollen.

[27] Wie bereits in der Einleitung erwähnt, siehe Stellungnahme 9/2014 der Artikel-29-Datenschutzgruppe zur Anwendung der Datenschutzrichtlinie für elektronische Kommunikation auf die Nutzung des virtuellen Fingerabdrucks.

Netzverbindung herstellen, um zu einem späteren Zeitpunkt Informationen zu übermitteln, würde dies einen „Zugriff“ im Sinne von Artikel 5 Absatz 3 ePrivacy-RL darstellen.

46. Für Untergruppen dieser Kategorien, die von besonderem Interesse sind- sei es aufgrund ihrer weiten Verbreitung oder weil eine spezifische Untersuchung im Hinblick auf die Umstände ihrer Verwendung gerechtfertigt ist - wird nachstehend eine spezifische Analyse vorgenommen.

3.1 URL- und Pixel-Tracking

47. Ein Tracking-Pixel ist ein Hyperlink zu einer Ressource, in der Regel einer Bilddatei, die in einen Inhalt wie eine Website oder eine E-Mail eingebettet ist. Solche Pixel erfüllen in der Regel keinen Zweck, der mit dem angeforderten Inhalt selbst zusammenhängt; sein einziger Zweck besteht darin, automatisch eine Kommunikation zwischen dem Client und dem Host des Pixels herzustellen, die andernfalls nicht stattgefunden hätte. Dies ist jedoch nicht systematisch der Fall, und Tracking-Pixel können auch durch Hinzufügen zusätzlicher Informationen zu Hyperlinks eingebetteter Bilder erstellt werden, die für den dem Nutzer angezeigten Inhalt relevant sind. Die Herstellung der Kommunikation selbst übermittelt je nach konkretem Anwendungsfall verschiedene Informationen an den Host des Pixels.

48. Auch in eine E-Mail kann der Absender ein Tracking-Pixel einfügen, um zu erkennen, wann der Empfänger die E-Mail liest. Tracking-Pixel auf Websites können mit einer Stelle verknüpft werden, die mehrere solcher Anfragen erfasst und somit in der Lage ist, das Verhalten der Nutzer zu verfolgen. Solche Tracking-Pixel können auch zusätzliche Kennungen, Metadaten oder Inhalte als Teil der Verknüpfung enthalten. Diese Datenpunkte können vom Betreiber der Website hinzugefügt und dabei potentiell im Zusammenhang mit der Aktivität des Nutzers auf der Website erstellt werden, um analytische Nutzungsberichte zu generieren. Sie können auch dynamisch durch clientseitige Anwendungslogik erzeugt werden, die von der Stelle bereitgestellt wird.

49. Tracking-Links können auf die gleiche Weise funktionieren, wobei hier die Kennung der Website-Adresse beigefügt wird. Wenn der Nutzer den Uniform Resource Locator (URL) aufruft, lädt die betreffende Website die angeforderte Ressource, erfasst dabei aber gleichzeitig auch eine Kennung, welche für die Identifizierung der Ressource nicht relevant ist. Sie werden von E-Commerce-Websites sehr häufig verwendet, um den Ursprung ihres ankommenden Datenverkehrs zu ermitteln. Solche Websites können beispielsweise Partnern Tracking-Links zur Verfügung stellen, die sie auf ihrer Domain verwenden können, so dass die E-Commerce-Website weiß, welcher ihrer Partner für einen Verkauf verantwortlich ist und eine Provision zahlt. Diese Praxis ist auch als „Affiliate-Marketing“ bekannt.

50. Sowohl Tracking-Links als auch Tracking-Pixel können über eine Vielzahl von Kanälen verbreitet werden, z. B. über E-Mails, Webseiten oder im Fall von Tracking-Links auch über jedwede Art von Textnachrichtensystemen. Diese Weitergabe an das Endgerät des Nutzers stellt eine Speicherung dar, zumindest durch den Caching-Mechanismus der clientseitigen Software. Daher findet Artikel 5 Absatz 3 ePrivacy-RL Anwendung, auch wenn es sich nicht um eine dauerhafte Speicherung handelt.

51. Die Hinzufügung von Tracking-Informationen zu URLs oder Bildern (Pixeln), die an den Nutzer gesendet werden, stellt eine Anweisung an das Endgerät dar, die gezielten Informationen (die angegebene Kennung) zurückzusenden. Bei dynamisch konstruierten Tracking-Pixeln stellt die Verbreitung der Anwendungslogik Logik (in der Regel JavaScript-Code) die Anweisung dar. Folglich kann davon ausgegangen werden, dass die Erfassung von Kennungen, die über solche Tracking-Mechanismen bereitgestellt werden, einen „Zugriff“ im Sinne von Artikel 5 Absatz 3 ePrivacy-RL darstellt und dieser somit auch für diesen Schritt gilt.

3.2 Lokale Verarbeitung

52. Einige Technologien stützen sich auf lokale Verarbeitungen, die durch auf den Endgeräten der Nutzer verbreitete Software gesteuert werden und die durch die lokale Verarbeitung erzeugten Informationen ausgewählten Akteuren über eine clientseitige API zur Verfügung stellen. Dies kann beispielsweise bei einer vom Webbrowser bereitgestellten API der Fall sein, bei der lokal generierte Ergebnisse aus der Ferne abgerufen werden können.

53. Wenn die verarbeiteten Informationen zu irgendeinem Zeitpunkt, beispielsweise im clientseitigem Programmcode einem Dritten zur Verfügung gestellt werden (diese z. B. über das Netzwerk an einen Server zurückgesandt werden) würde ein solcher Vorgang (auf Anweisung der Stelle, die den auf dem Endgerät des Nutzers verbreiteten clientseitigen Programmcode herstellt) einen „Zugriff auf bereits gespeicherte Informationen“ darstellen. Die Tatsache, dass diese Informationen lokal erstellt werden, schließt die Anwendung von Artikel 5 Absatz 3 ePrivacy-RL nicht aus.

3.3 Tracking nur auf der Grundlage der IP-Adresse

54. Einige Anbieter entwickeln Lösungen, die sich nur auf die Erfassung einer Komponente stützen, nämlich der IP-Adresse, um die Navigation[28] des Nutzers zu verfolgen, in einigen Fällen über mehrere Domänen hinweg. In diesem Zusammenhang könnte Artikel 5 Absatz 3 ePrivacy-RL Anwendung finden, auch wenn die Anweisung, die IP-Adresse bereitzustellen, von einer anderen Stelle als der empfangenden Stelle erteilt wurde.

55. Der Zugriff auf IP-Adressen würde jedoch nur dann die Anwendung von Artikel 5 Absatz 3 ePrivacy-RL auslösen, wenn diese Informationen vom Endgerät eines Teilnehmers oder Nutzers stammen. Dies ist zwar nicht systematisch der Fall (z. B. wenn CGNAT[29] aktiviert ist), aber die statischen ausgehenden IPv4-Adressen die vom Router eines Nutzers stammen, fallen darunter, ebenso wie IPv6-Adressen, da sie teilweise vom Host definiert werden. Solange die Stelle nicht sicher ausschließen kann, dass die IP-Adresse vom Endgerät eines Nutzers oder Teilnehmers stammt, muss sie alle Maßnahmen gemäß Artikel 5 Absatz 3 ePrivacy-RL ergreifen.

56. Auch wenn in den vorliegenden Leitlinien die Anwendung der in Artikel 5 Absatz 3 ePrivacy-RL vorgesehenen Ausnahmen von der Verpflichtung zur Einholung der Einwilligung nicht untersucht wird, ist es doch wichtig, erneut darauf hinzuweisen, dass die Anwendbarkeit dieses Artikels nicht systematisch bedeutet, dass eine Einwilligung eingeholt werden muss. Der EDSA erinnert daher daran, dass in jedem Fall zu prüfen wäre, ob eine Einwilligung erforderlich ist oder ob eine Ausnahme nach Artikel 5 Absatz 3 ePrivacy-RL gelten könnte[30].

3.4 Intermittierende und vermittelte Meldung über das Internet der Dinge

57. IoT-Geräte (Internet der Dinge) erzeugen im Laufe der Zeit kontinuierlich Informationen, z. B. durch im Gerät eingebettete Sensoren, die lokal vorverarbeitet werden können oder nicht. In vielen Fällen

[28] Dies gilt zusätzlich zu und unabhängig von der Verwendung und Funktion einer IP-Adresse für die Erstellung und Übertragung oder Übermittlung zugrundeliegender technischer Mitteilungen oder der Tatsache, dass es sich bei dieser Adresse um personenbezogene Daten handeln kann oder nicht (bei der Analyse des Datenschutzes in der elektronischen Kommunikation handelt es sich um „Informationen“).

[29] Carrier-Grade NAT oder CGNAT wird von Internetdienstanbietern verwendet, um die Nutzung des begrenzten IP-Adressraums zu maximieren. Es fasst eine Reihe von Abonnenten unter derselben öffentlichen IP-Adresse zusammen.

[30] Die WP29-Stellungnahme 9/2014 enthält einige Beispiele für Fälle, in denen eine Einwilligung nicht erforderlich sein könnte.

werden Informationen einem entfernten Server zur Verfügung gestellt, aber die Modalitäten dieser Erhebung können variieren.

58. Einige IoT-Geräte haben eine direkte Verbindung zu einem öffentlichen Kommunikationsnetz durch eine Mobilfunk SIM-Karte. Andere können eine indirekte Verbindung zu einem öffentlichen Kommunikationsnetz haben, z. B. durch die Nutzung von WLAN oder die Weitergabe von Informationen an ein anderes Gerät über eine Punkt-zu-Punkt-Verbindung (z. B. über Bluetooth). Bei dem anderen Gerät kann es sich beispielsweise um ein Smartphone oder ein spezielles Gateway handeln, das die Informationen vor der Übermittlung an den Server vorab verarbeiten kann oder nicht.

59. IoT-Geräte könnten vom Hersteller angewiesen werden, die gesammelten Informationen immer zu übermitteln (streamen), sie aber dennoch zunächst lokal zwischenzuspeichern, zum Beispiel bis eine Verbindung verfügbar ist.

60. In jedem Fall würde das IoT-Gerät, wenn es (direkt oder indirekt) an ein öffentliches Kommunikationsnetz angeschlossen ist, selbst als Endgerät betrachtet werden. Die Tatsache, dass die Informationen gestreamt oder für eine intermittierende Meldung zwischengespeichert werden, ändert nichts an der Art dieser Informationen. In beiden Fällen würde Artikel 5 Absatz 3 ePrivacy-RL gelten, da durch die Anweisung eines Programmcodes auf dem IoT-Gerät, die dynamisch gespeicherten Daten an den entfernten Server zu senden, ein „Zugriff“ erfolgt.

3.5 Eindeutige Kennungen

61. Ein von Unternehmen häufig verwendetes Instrument ist das Konzept der „eindeutigen Kennungen“ oder „dauerhaften Kennungen“. Solche Kennungen können aus dauerhaften personenbezogenen Daten (Vor- und Nachname, E-Mail, Telefonnummer usw.) abgeleitet werden, welche auf dem Endgerät des Nutzers gehasht und von mehreren Verantwortlichen gesammelt und weitergegeben werden, um eine Person über verschiedene Datensätze hinweg eindeutig zu identifizieren (Nutzungsdaten, die durch die Nutzung einer Website oder Anwendung gesammelt werden, CRM-Daten (Customer Relationship Management) im Zusammenhang mit einem Online- oder Offline-Kauf oder -Abonnement usw.). Auf Websites werden die dauerhaften personenbezogenen Daten im Allgemeinen im Rahmen der Authentifizierung oder des Abonnements von Newslettern erhoben.

62. Wie bereits dargelegt, würde die Tatsache, dass Informationen vom Nutzer eingegeben werden, die Anwendung von Artikel 5 Absatz 3 ePrivacy-RL in Bezug auf die Speicherung nicht ausschließen, da diese Informationen vorübergehend im Endgerät gespeichert werden, bevor sie erfasst werden.

63. Im Zusammenhang mit der Erfassung von „eindeutigen Kennungen“ auf Websites oder in mobilen Anwendungen weist die erfassende Stelle den Browser (durch die Verbreitung von clientseitigem Programmcode) an, diese Informationen zu senden. Es erfolgt also ein „Zugriff“, und Artikel 5 Absatz 3 ePrivacy-RL findet Anwendung.