Riktlinjer

Riktlinjer 2/2023 om det tekniska tillämpningsområdet för artikel 5.3 i direktivet om integritet och elektronisk kommunikation

Version 2.0

Antagna den 7 oktober 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Versionshistorik

Version 1.0	14 november 2022	Antagande av riktlinjerna inför offentligt samråd
Version 2.0	7 oktober 2024	Antagande av riktlinjerna efter offentligt samråd

Sammanfattning

I dessa riktlinjer behandlar Europeiska dataskyddsstyrelsen (EDPB) tillämpningen av artikel 5.3 i direktivet om integritet och elektronisk kommunikation på olika tekniska lösningar. Dessa riktlinjer bygger vidare på yttrande 9/2014 från artikel 29-gruppen om tillämpningen av direktivet om integritet och elektronisk kommunikation på signaturinsamling och syftar till att ge en tydlig förståelse för de tekniska åtgärder som omfattas av artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

Uppkomsten av nya spårningsmetoder för att både ersätta befintliga spårningsverktyg (t.ex. kakor, på grund av att vissa leverantörer av webbläsare har slutat ge stöd för tredjepartskakor) och skapa nya affärsmodeller har blivit ett allvarligt problem för uppgiftsskyddet. Även om tillämpligheten av artikel 5.3 i direktivet om integritet och elektronisk kommunikation är väl etablerad och genomförd för viss spårningsteknik, såsom kakor, finns det ett behov av att ta itu med tvetydigheter i samband med tillämpningen av denna bestämmelse på framväxande spårningsverktyg.

I riktlinjerna identifieras tre centrala aspekter för tillämpligheten av artikel 5.3 i direktivet om integritet och elektronisk kommunikation (avsnitt 2.1), nämligen ”information”, ”abonnentens eller användarens terminalutrustning” och ”få tillgång till och lagring av information och lagrad information”. Riktlinjerna innehåller vidare en detaljerad analys av varje aspekt (avsnitt 2.2–2.6).

I avsnitt 3 tillämpas denna analys på en icke uttömmande förteckning över användningsfall som representerar vanliga tekniker, nämligen

- URL- och pixelspårning,
- lokal behandling,
- spårning baserad endast på IP-adress,
- intermittent och förmedlad rapportering via sakernas internet,
- unik identifierare.

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit dessa riktlinjer

med beaktande av artikel 70.1 e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan kallad *den allmänna dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artikel 15.3 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation, ändrat genom direktiv 2009/136/EG (nedan kallat *direktivet om integritet och elektronisk kommunikation*), och

med beaktande av artikel 12 och artikel 22 i arbetsordningen.

HÄRIGENOM FÖRESKRIVS FÖLJANDE:

1 INLEDNING

1. Enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation är ”lagring av information eller tillgång till information som redan är lagrad i en abonnents eller användares terminalutrustning” endast tillåtet på grundval av samtycke eller nödvändighet för specifika ändamål som anges i den artikeln. Som påpekas i skäl 24 i direktivet om integritet och elektronisk kommunikation[2] är syftet med den bestämmelsen att skydda användarnas terminalutrustning, eftersom den är en del av användarnas privatliv. Det framgår av lydelsen att artikel 5.3 i direktivet om integritet och elektronisk kommunikation inte enbart gäller för kakor, utan även för ”liknande teknik”. Det finns dock för närvarande ingen uttömmande förteckning över de tekniska åtgärder som omfattas av artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

2. Artikel 29-gruppens yttrande 9/2014 om tillämpningen av direktivet om integritet och elektronisk kommunikation på fingeravtryck (nedan kallat *artikel 29-gruppens yttrande 9/2014*) har redan klargjort att signaturinsamling omfattas av det tekniska tillämpningsområdet för artikel 5.3 i direktivet om integritet och elektronisk kommunikation[3], men på grund av de nya tekniska framstegen behövs ytterligare vägledning när det gäller den spårningsteknik som för närvarande observeras. Det tekniska landskapet har utvecklats under det senaste årtiondet, med den ökande användningen av identifierare

[1] Hänvisningar till ”medlemsstater” i detta dokument ska tolkas som hänvisningar till ”EES-medlemsstater”.
[2] ”Terminalutrustning för användare av elektroniska kommunikationsnät och all information som finns lagrad i sådan utrustning är en del av privatlivet för användarna och kräver skydd enligt Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Sådana anordningar som ’spyware’, ’web bugs’, hemliga identifieringsuppgifter och liknande som ger tillträde till användarnas terminaler utan deras kännedom, för att få tillgång till information, lagra hemlig information eller spåra användarnas verksamhet, kan allvarligt inkräkta på dessa användares integritet. Användning av sådana anordningar bör tillåtas endast för legitima syften och med de berörda användarnas kännedom.”
[3] Artikel 29-gruppens yttrande 9/2014, s. 11.

som är inbyggda i operativsystem, samt skapandet av nya verktyg som gör det möjligt att lagra information i terminalutrustning.

3. Oklarheterna kring tillämpningsområdet för artikel 5.3 i direktivet om integritet och elektronisk kommunikation har skapat incitament för att genomföra alternativa lösningar för att spåra internetanvändare och leder till en tendens att kringgå de rättsliga skyldigheter som föreskrivs i artikel 5.3 i direktivet om integritet och elektronisk kommunikation. Alla sådana situationer ger anledning till oro och kräver en kompletterande analys för att komplettera den tidigare vägledningen från EDPB.

4. Syftet med dessa riktlinjer är att göra en teknisk analys av tillämpningsområdet för artikel 5.3 i direktivet om integritet och elektronisk kommunikation, nämligen att klargöra vad som tekniskt sett omfattas av uttrycket ”lagring av information eller tillgång till information som redan är lagrad i en abonnents eller användares terminalutrustning”. Dessa riktlinjer behandlar inte de omständigheter under vilka en behandling kan omfattas av de undantag från kravet på samtycke som anges i direktivet om integritet och elektronisk kommunikation[4], eftersom dessa omständigheter bör analyseras från fall till fall med beaktande av relevanta införlivanden i medlemsstaterna och vägledning som utfärdats av nationella behöriga myndigheter.

5. En icke uttömmande förteckning över specifika användningsfall kommer att analyseras i den sista delen av dessa riktlinjer.

2 ANALYS

2.1 Centrala aspekter för tillämpligheten av artikel 5.3 i direktivet om integritet och elektronisk kommunikation

6. Artikel 5.3 i direktivet om integritet och elektronisk kommunikation är tillämplig om följande kriterier är uppfyllda:

   a. **KRITERIUM A:** De åtgärder som vidtas avser ”information”. Det bör noteras att den term som används inte är ”personuppgifter” utan ”information”.

   b. **KRITERIUM B:** den verksamhet som bedrivs omfattar en ”terminalutrustning” som tillhör en abonnent eller användare (B.1), vilket innebär att det är nödvändigt att bedöma begreppet ”allmänt kommunikationsnät” (B.2).

   c. **KRITERIUM C** de utförda transaktionerna utgör verkligen ”lagring” (C.1) eller ”tillgång” (C.2). Dessa två begrepp kan studeras oberoende av varandra, vilket påminns om i artikel 29-gruppens yttrande 9/2014: ”Orden ’uppgifter som lagras eller ges åtkomst till’ anger att lagring och åtkomst inte behöver ske inom samma kommunikation och inte behöver utföras av samma part”[5].

   För läsbarhetens skull kommer den enhet som får tillgång till information som lagras i användarens terminalutrustning nedan att kallas en ”åtkomstenhet”.

[4] I artikel 5.3 i direktivet om integritet och elektronisk kommunikation anges följande: ”Detta får inte förhindra någon teknisk lagring eller åtkomst som endast sker för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller det som är absolut nödvändigt för att leverantören ska kunna tillhandahålla en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt.”

[5] Artikel 29-gruppens yttrande 9/2014, s. 8.

2.2 Begreppet ”information” – kriterium A

7. I enlighet med vad som anges i KRITERIUM A beskrivs i detta avsnitt vad som omfattas av begreppet ”information”. Valet av termen ”information”, som omfattar en bredare kategori än enbart begreppet personuppgifter, hänger samman med tillämpningsområdet för direktivet om integritet och elektronisk kommunikation.

8. Syftet med artikel 5.3 i direktivet är att skydda användarnas privatliv, vilket anges i skäl 24: ”Terminalutrustning för användare av elektroniska kommunikationsnät och all information som finns lagrad i sådan utrustning är en del av privatlivet för användarna och kräver skydd enligt Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.” Det skyddas också av artikel 7 i EU:s stadga om de grundläggande rättigheterna.

9. Scenarier som inkräktar på privatlivet även om de inte innehåller några personuppgifter omfattas i själva verket uttryckligen av ordalydelsen i artikel 5.3 och skäl 24 i direktivet om integritet och elektronisk kommunikation, t.ex. lagring av virus på användarens terminalutrustning. Detta visar att definitionen av begreppet ”information” inte bör begränsas till egenskapen att ha en koppling en identifierad eller identifierbar fysisk person.

10. Detta har bekräftats av EU-domstolen: ”Detta skydd gäller all information som finns lagrad på denna terminalutrustning, oavsett om det rör sig om personuppgifter eller inte och, såsom framgår av samma skäl, syftar till att bland annat skydda användarna mot riskerna med hemliga identifieringsuppgifter eller liknande som ger tillträde till användarnas terminalutrustning utan deras kännedom.”[6]

11. Frågorna om huruvida ursprunget till denna information och skälen till varför den lagras i terminalutrustningen ska beaktas vid bedömningen av tillämpligheten av artikel 5.3 i direktivet om integritet och elektronisk kommunikation har klargjorts tidigare. Till exempel i artikel 29-gruppens yttrande 9/2014: ”Detta ska dock inte tolkas som att den tredje parten inte behöver samtycke för att få åtkomst till informationen bara för att den inte har lagrat uppgifterna. Samtyckeskravet gäller även när åtkomst ges till ett ’read-only’-värde (t.ex. en begäran om MAC-adressen för ett nätverksgränssnitt via OS API).”[7].

12. Sammanfattningsvis omfattar begreppet information både icke-personuppgifter och personuppgifter, oavsett hur dessa uppgifter lagrades och av vem, dvs. av en extern enhet (även inbegripet andra enheter än den som har åtkomst), av användaren, av en tillverkare eller på något annat sätt.

2.3 Begreppet ”en abonnents eller användares terminalutrustning” – kriterium B.1

13. Detta avsnitt bygger på den definition som används i direktiv 2008/63/EG och som det hänvisas till i artikel 2 i direktiv (EU) 2018/1972, där ”terminalutrustning” definieras som ”utrustning direkt eller indirekt ansluten till en nätanslutningspunkt i ett allmänt tillgängligt telenät för att sända, bearbeta eller ta emot information; i ettdera fallet (direkt eller indirekt) kan anslutningen göras med tråd, optisk fiber eller elektromagnetiskt; en anslutning är indirekt om utrustningen är placerad mellan terminalutrustningen och nätanslutningspunkten”.[8]

14. Skäl 24 i direktivet om integritet och elektronisk kommunikation ger en tydlig förståelse av terminalutrustningens roll för det skydd som erbjuds genom artikel 5.3 i direktivet om integritet och

[6] Domstolens dom av den 1 oktober 2019, Planet 49, mål C-673/17, ECLI:EU:C:2019:801, punkt 70.
[7] Artikel 29-gruppens yttrande 9/2014, s. 8.
[8] Kommissionens direktiv 2008/63/EG av den 20 juni 2008 om konkurrens på marknaderna för teleterminalutrustning (kodifierad version), artikel 1.1.

elektronisk kommunikation. Direktivet om integritet och elektronisk kommunikation skyddar användarnas integritet inte bara i förhållande till sekretessen för deras uppgifter utan också genom att skydda integriteten hos användarens terminalutrustning. Denna förståelse kommer att vägleda tolkningen av begreppet terminalutrustning i dessa riktlinjer.

15. I artikel 3 i direktivet om integritet och elektronisk kommunikation anges att för att direktivet ska vara tillämpligt måste behandlingen av personuppgifter utföras i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät. Detta innebär att en anordning ska kunna användas i samband med en sådan tjänst och att den, för att betecknas som terminalutrustning, ska vara ansluten eller kunna anslutas[9] till gränssnittet för ett allmänt kommunikationsnät. EDPB konstaterar att de ändringar som gjordes 2009[10] i lydelsen av artikel 5.3 i direktivet om integritet och elektronisk kommunikation utvidgade skyddet av terminalutrustning genom att hänvisningen till ”användningen av elektroniska kommunikationsnät” som ett sätt att lagra information eller få tillgång till information lagrad i terminalutrustningen togs bort. Så länge en anordning har ett nätverksgränssnitt som gör den berättigad till anslutning (även om en sådan anslutning inte är på plats) gäller därför artikel 5.3 i direktivet om integritet och elektronisk kommunikation för alla enheter som skulle lagra och få tillgång till information som redan finns lagrad i terminalutrustningen, oavsett medel för åtkomst till terminalutrustningen, och oavsett om den är ansluten till eller bortkopplad från ett nät.

16. Utrustning som ingår i det allmänna elektroniska kommunikationsnätet i sig skulle inte betraktas som terminalutrustning enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation[11].

17. En terminalutrustning kan bestå av ett valfritt antal enskilda delar av hårdvara, som tillsammans bildar terminalutrustningen. Det kan röra sig om en fysiskt innesluten enhet som innehåller all hårdvara för visning, bearbetning, lagring och kringutrustning (t.ex. smarta telefoner, bärbara datorer, nätverksanslutna lagringsenheter, uppkopplade bilar eller uppkopplade tv-apparater, smarta glasögon).

18. I direktivet erkänns att skyddet av konfidentialiteten för den information som lagras på en användares terminalutrustning och integriteten hos användarens terminalutrustning inte är begränsat till skyddet av fysiska personers privatliv, utan även avser rätten till respekt för deras korrespondens eller juridiska personers legitima intressen[12]. En terminalutrustning som möjliggör denna korrespondens och de juridiska personernas legitima intressen skyddas därför enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

19. Användaren eller abonnenten kan äga eller hyra eller på annat sätt få tillgång till terminalutrustningen. Flera användare eller abonnenter kan dela samma terminalutrustning.

---

[9] Det vill säga att de har den tekniska kapacitet som krävs för att anslutas till nätverket även om den anslutningen ännu inte har inrättats.

[10] Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om samarbete mellan de nationella tillsynsmyndigheter som ansvarar för konsumentskyddslagstiftningen (Text av betydelse för EES), EUT L 337, 18.12.2009, artikel 2.5 och skäl 65.

[11] För att identifiera gränserna för nätverket i olika sammanhang, se Berecs riktlinjer för gemensamma strategier för identifiering av nätanslutningspunkten i olika nättopologier (BoR (20) 46).

[12] Såsom påpekas i artikel 2.13 i Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation kan användaren vara en fysisk eller juridisk person.

20. Detta skydd garanteras genom direktivet om integritet och elektronisk kommunikation för den terminalutrustning som är kopplad till användaren eller abonnenten, och det är inte beroende av om användaren ställer upp åtkomstmedlen (t.ex. om de initierade den elektroniska kommunikationen) eller ens om användaren är medveten om dessa åtkomstmedel.

2.4 Begreppet ”allmänt kommunikationsnät” – kriterium B.2

21. Eftersom den situation som regleras i direktivet om integritet och elektronisk kommunikation är den som rör ”allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom gemenskapen”[13], och definitionen av terminalutrustning uttryckligen nämner begreppet ”allmänt kommunikationsnät”, är det mycket viktigt att klargöra detta begrepp för att identifiera det sammanhang i vilket artikel 5.3 i direktivet är tillämplig.

22. Begreppet elektroniskt kommunikationsnät definieras inte i själva direktivet om integritet och elektronisk kommunikation. Det hänvisades ursprungligen till det begreppet i direktiv 2002/21/EG (ramdirektivet) om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster[14], senare ersatt av artikel 2.1 i direktiv 2018/1972 (den europeiska kodexen för elektronisk kommunikation). Texten har nu följande lydelse:

> elektroniskt kommunikationsnät*: system för överföring, oberoende av om det bygger på en permanent infrastruktur eller en centralt administrerad kapacitet eller inte, och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser, inbegripet nätelement som inte är aktiva, som medger överföring av signaler via tråd, via radio, på optisk väg eller via andra elektromagnetiska överföringsmedier, däribland satellitnät, fasta nät (kretskopplade och paketkopplade, inbegripet internet) och mobilnät, elnätssystem i den utsträckning dessa används för signalöverföring, nät för radio- och tv-utsändning samt kabel-tv-nät, oberoende av vilken typ av information som överförs*[15].

23. Denna definition är neutral med avseende på överföringsteknik. Ett elektroniskt kommunikationsnät är enligt denna definition varje nätsystem som möjliggör överföring av elektroniska signaler mellan dess noder, oavsett vilken utrustning och vilka protokoll som används.

24. Begreppet elektroniskt kommunikationsnät enligt direktiv 2018/1972 beror inte på infrastrukturens offentliga eller privata karaktär eller på hur nätet sätts in eller förvaltas (”oberoende av om det bygger på en permanent infrastruktur eller en centralt administrerad kapacitet eller inte”[16]). Till följd av detta är definitionen av elektroniska kommunikationsnät, enligt artikel 2 i direktiv 2018/1972, tillräckligt bred för att omfatta alla typer av infrastruktur. Det omfattar nätverk som förvaltas eller inte förvaltas av en operatör, nätverk som förvaltas gemensamt av en grupp operatörer, eller till och med ad hoc-nätverk där en terminalutrustning på ett dynamiskt sätt kan anslutas till eller lämna ett nät av annan terminalutrustning som använder protokoll för kortdistanskommunikation.

25. I denna definition av nätverk anges ingen begränsning när det gäller mängden terminalutrustning som finns i nätverket vid någon tidpunkt. Vissa nätverkssystem bygger på att noder vidarebefordrar

[13] Artikel 3 i direktivet om integritet och elektronisk kommunikation.

[14] Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv).

[15] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) (Text av betydelse för EES), artikel 2.1.

[16] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) (Text av betydelse för EES), artikel 2.1.

information ad hoc till noder som är uppkopplade vid den tidpunkten[17] och kan vid en viss tidpunkt ha så lite som två element som kommunicerar. Sådana fall skulle omfattas av det allmänna tillämpningsområdet för direktivet om integritet och elektronisk kommunikation, så länge nätverksprotokollet tillåter ytterligare inkludering av jämlika element.

26. Kommunikationsnätets allmänna tillgänglighet är nödvändig för att enheten ska betraktas som terminalutrustning och följaktligen för tillämpligheten av artikel 5.3 i direktivet om integritet och elektronisk kommunikation. Det bör noteras att den omständigheten att nätverket görs tillgängligt för en begränsad del av allmänheten (till exempel abonnenter, oavsett om de betalar eller inte, under förutsättning att behörighetsvillkoren är uppfyllda) inte innebär att ett sådant nätverk är privat[18].

2.5 Begreppet ”få tillgång till” – kriterium C.1

27. För att korrekt definiera begreppet ”få tillgång till” är det viktigt att beakta direktivets tillämpningsområde, som anges i artikel 1: ”[A]tt säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, samt för att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom gemenskapen”.

28. I korthet är direktivet om integritet och elektronisk kommunikation ett integritetsbevarande rättsligt instrument som syftar till att skydda kommunikationens konfidentialitet och enheternas integritet. I skäl 24 i direktivet klargörs att när det gäller fysiska personer utgör användarens terminalutrustning en del av deras privatliv och att tillgång till information som lagras på den utan deras vetskap allvarligt kan inkräkta på deras integritet.

29. Juridiska personer skyddas också av direktivet om integritet och elektronisk kommunikation[19]. Följaktligen måste begreppet ”få tillgång till” enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation tolkas på ett sätt som skyddar dessa rättigheter mot intrång från tredje part.

30. Lagring av eller tillgång till information kan vara oberoende operationer som utförs av oberoende enheter. Lagring av information och tillgång till information som redan har lagrats behöver inte förekomma samtidigt för att artikel 5.3 i direktivet om integritet och elektronisk kommunikation ska vara tillämplig.

31. Såsom noterades i artikel 29-gruppens yttrande 9/2014: ”Orden ’uppgifter som lagras eller ges åtkomst till’ anger att lagring och åtkomst inte behöver ske inom samma kommunikation och inte behöver utföras av samma part. Uppgifter som lagras av en part (inklusive uppgifter som lagras av användaren eller produkttillverkaren) och som en annan part senare får åtkomst till omfattas därför av artikel 5.3.”[20] Följaktligen finns det inga begränsningar för informationens ursprung i terminalutrustningen för att begreppet tillgång ska vara tillämpligt.

32. Närhelst en enhet vidtar åtgärder för att få tillgång till information som lagras i terminalutrustningen skulle artikel 5.3 i direktivet om integritet och elektronisk kommunikation vara tillämplig. Vanligtvis innebär detta att åtkomstenheten proaktivt skickar specifika instruktioner till terminalutrustningen för

[17] Till exempel i samband med fördröjningstoleranta nätverkssystem som implementerar ”lagra- och vidarebefordra-tekniker”, såsom Briar-projektet med öppen källkod.
[18] För en närmare analys av identifieringen av allmänna kommunikationsnät hänvisas till Berecs riktlinjer för genomförandet av förordningen om ett öppet internet (BoR (20) 112).
[19] Skäl 26 i direktivet om integritet och elektronisk kommunikation, se punkt 17 ovan.
[20] Artikel 29-gruppens yttrande 9/2014, s. 8.

att få tillbaka den avsedda informationen. Detta gäller t.ex. kakor, där åtkomstenheten instruerar terminalutrustningen att proaktivt skicka information vid varje efterföljande anrop till HTTP-protokollet (Hypertext Transfer Protocol).

33. Detta är också fallet när åtkomstenheten distribuerar programvara till användarens terminalutrustning som lagras och sedan proaktivt anropar en API-slutpunkt (Application Programming Interface, programmeringsgränssnitt) via nätet. Ytterligare exempel kan vara JavaScript-kod, där åtkomstenheten instruerar användarens webbläsare att skicka asynkrona förfrågningar med den riktade informationen. Sådan åtkomst faller tydligt inom tillämpningsområdet för artikel 5.3 i direktivet om integritet och elektronisk kommunikation, eftersom åtkomstenheten uttryckligen instruerar terminalutrustningen att skicka informationen.

34. I vissa fall kan det hända att den enhet som instruerar terminalutrustningen att skicka tillbaka de berörda uppgifterna är en annan än den enhet som tar emot informationen. Detta kan vara en följd av tillhandahållandet och/eller användningen av en gemensam mekanism mellan de båda enheterna. Att instruera enheten att sända redan lagrad information (till exempel genom användning av ett protokoll eller ett programvaruutvecklingsverktyg[21] som innebär att terminalutrustningen proaktivt skickar information) gör det möjligt att göra intrång i terminalutrustningen, vilket innebär att en sådan tillgång uppfyller kriterierna för att artikel 5.3 i direktivet om integritet och elektronisk kommunikation ska vara tillämplig. Såsom påpekas i artikel 29-gruppens yttrande 9/2014 kan detta vara fallet när en webbplats instruerar terminalutrustningen att skicka information till tredje parts reklamtjänster genom att inkludera en spårningspixel[22]. Detta användningsfall vidareutvecklas i avsnitt 3.1.

2.6 Begreppen ”lagring av information” och ”lagrad information” – kriterium C.2

35. Lagring av information i den mening som avses i artikel 5.3 i direktivet om integritet och elektronisk kommunikation innebär att information placeras på ett fysiskt elektroniskt lagringsmedium som ingår i en användares eller abonnents terminalutrustning[23].

36. Vanligtvis lagras inte information i en användares eller abonnents terminalutrustning genom direkt tillgång till anordningens minne av en annan part, utan snarare genom att programvaran på terminalutrustningen instrueras att generera specifik information. Lagring som sker genom sådana instruktioner anses initieras direkt av den andra parten. Detta innefattar användning av etablerade protokoll såsom lagring av kakor i webbläsare samt anpassad programvara, oavsett vem som skapat eller installerat protokollen eller programvaran på terminalutrustningen.

37. I direktivet om integritet och elektronisk kommunikation anges inte någon övre eller nedre gräns för hur länge information måste finnas kvar på ett lagringsmedium för att räknas som lagrad, och det finns inte heller någon övre eller nedre gräns för hur mycket information som ska lagras.

38. På samma sätt är begreppet lagring inte beroende av vilken typ av medium som informationen lagras på. Typiska exempel är hårddiskar (HDD), SSD-minnen (Solid State Drive), elektriskt raderbara programmerbara skrivminnen (EEPROM) och RAM-minnen (Random Access Memory), men mer ovanliga lösningar med medier som magnetband eller cacheminne för en central processorenhet (CPU) är inte uteslutna från tillämpningsområdet. Lagringsmediet kan anslutas internt (t.ex. genom en SATA-anslutning) eller externt (t.ex. genom en USB-anslutning).

[21] Ett programvaruutvecklingsverktyg är ett paket med verktyg för utveckling av programvara som görs tillgängligt för att underlätta skapandet av applikationsprogramvara.
[22] Artikel 29-gruppens yttrande 9/2014, s. 9.
[23] Enligt definitionen i avsnitt 2.3 i dessa riktlinjer.

39. Med ”lagrad information” avses information som redan finns på terminalutrustningen, oavsett källan till eller arten av denna information. Detta inbegriper alla resultat från lagring av information i den mening som avses i artikel 5.3 i direktivet om integritet och elektronisk kommunikation enligt beskrivningen ovan (antingen av samma part som senare skulle få tillgång till informationen eller av en annan tredje part). Det omfattar även resultat av informationslagringsprocesser som ligger utanför tillämpningsområdet för artikel 5.3 i direktivet om integritet och elektronisk lagring, t.ex. lagring i terminalutrustningen av användaren eller abonnenten själv eller av en hårdvarutillverkare (t.ex. MAC-adresser för nätverksgränssnittskontroller), sensorer som är integrerade i terminalutrustningen eller processer och program som körs i terminalutrustningen, som eventuellt producerar information som är beroende av eller härrör från lagrad information.

3 ANVÄNDNINGSFALL

40. Såsom påpekas i inledningen till dessa riktlinjer[24] görs ingen analys av tillämpningen av undantagen från skyldigheten att inhämta samtycke enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation. EDPB påminner om att det i alla de fall där det förekommer lagring av information eller tillgång till redan lagrad information måste göras en bedömning av om samtycke behövs eller om ett undantag enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation skulle kunna tillämpas. Läsaren bör därför ta hänsyn till undantagen i sitt användningsfall, i samband med denna tekniska analys.

41. Utan att det påverkar det specifika sammanhang i vilket det går att använda de tekniska kategorier som är nödvändiga för att avgöra om artikel 5.3 i direktivet om integritet och elektronisk kommunikation är tillämplig, är det möjligt att på ett icke uttömmande sätt identifiera breda kategorier av identifierare och information som används allmänt och som kan omfattas av artikel 5.3 i det direktivet.

42. Nätverkskommunikationen bygger vanligtvis på en skiktad modell som kräver användning av identifierare för att kommunikationen ska kunna upprättas och genomföras korrekt. Instruktionen om att sända dessa identifierare till fjärraktörer görs genom programvara som följer överenskomna kommunikationsprotokoll. Att den mottagande enheten kanske inte är den enhet som ger instruktioner om översändande av information utesluter som sagt inte tillämpningen av artikel 5.3 i direktivet om integritet och elektronisk kommunikation. Detta kan gälla routingidentifierare såsom terminalutrustningens MAC- eller IP-adress, men även sessionsidentifierare (SSRC, Websocket identifier) eller autentiseringstoken.

43. På samma sätt kan applikationsprotokollet innehålla flera mekanismer för att tillhandahålla kontextdata (t.ex. ett HTTP-sidhuvud som innehåller ett godkännandefält eller en användaragent), en cachemekanism (t.ex. ETag[25]) eller andra funktioner (däribland kakor, eller HSTS[26]). Även användning av dessa mekanismer för att samla in information (t.ex. i samband med signaturinsamling[27] eller

[24] Se punkt 4.
[25] HTTP ETag är en identifierare som gör det möjligt att göra villkorsstyrda förfrågningar baserat på giltigheten hos cachelagrade klientdata.
[26] HTTP Strict Transport Security (HSTS) gör det möjligt för servrar att specificera vilka resurser som alltid bör begäras med hjälp av HTTPS-anslutningar.
[27] Se yttrande 9/2014 från artikel 29-gruppen om tillämpningen av direktivet om integritet och elektronisk kommunikation på digitala fingeravtryck.

spårning av resursidentifierare) kan leda till tillämpning av artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

44. Å andra sidan finns det vissa sammanhang där lokala tillämpningar som installerats i terminalutrustningen enbart använder viss information inuti terminalen. Detta kan t.ex. gälla API:er för smarttelefonsystem (åtkomst till kamera, mikrofon, GPS-sensor, acceleratorchipp, radiochipp, lokal filtillgång, kontaktlista, åtkomst till identifierare osv.). Detta kan också vara fallet för webbläsare som behandlar information som lagras eller genereras inuti enheten (t.ex. kakor, lokal lagring, WebSQL eller till och med information som tillhandahålls av användarna själva). Att sådan information används av en applikation skulle inte innebära att ”få tillgång till redan lagrad information” i den mening som avses i artikel 5.3 i direktivet om integritet och elektronisk kommunikation så länge informationen inte lämnar enheten. Om tillgång ges till denna information eller någon härledning av den skulle artikel 5.3 i det direktivet dock vara tillämplig.

45. Slutligen distribueras i vissa fall skadlig programvara av aktörer, t.ex. programvara för kryptokapning eller mer allmänt skadlig programvara, som utnyttjar terminalutrustningens processorkapacitet till förmån för den distribuerande aktören. Distributionen av den skadliga programvaran i användarens terminalutrustning skulle utgöra en ”lagring” i den mening som avses i artikel 5.3 i direktivet om integritet och elektronisk kommunikation. Om programvaran dessutom upprättar en nätverksanslutning för att skicka information i ett senare skede, skulle det vara att ”få tillgång” i den mening som avses i artikel 5.3 i direktivet om integritet och elektronisk kommunikation

46. För en undergrupp av dessa kategorier som är av särskilt intresse på grund av deras utbredda användning eller på grund av att en särskild studie är motiverad med hänsyn till omständigheterna för deras användning, görs en särskild analys nedan.

3.1 URL- och pixelspårning

47. En spårningspixel är en hyperlänk till en resurs, vanligtvis en bildfil, som är inbyggd i ett innehåll som en webbplats eller ett e-postmeddelande. Denna pixel uppfyller vanligtvis inget syfte som är relaterat till det begärda innehållet i sig. Dess enda syfte är att automatiskt upprätta en kommunikation från klienten till värden för pixeln, som annars inte skulle ha uppstått. Detta är dock inte systematiskt och spårningspixlar kan också skapas genom att ytterligare information läggs till bilder som laddas via hyperlänkar och som är relevanta för det innehåll som visas för användaren. Genom att kommunikationen upprättas överförs olika uppgifter till pixelns värd, beroende på det specifika användningsfallet.

48. Om det rör sig om ett e-postmeddelande kan avsändaren inkludera en spårningspixel för att upptäcka när mottagaren läser e-postmeddelandet. Spårningspixlar på webbplatser kan länka till en enhet som samlar in en mängd sådana förfrågningar och därmed kan spåra användarnas beteende. Sådana spårningspixlar kan också innehålla ytterligare identifierare, metadata eller innehåll som en del av länken. Dessa datapunkter kan läggas till av webbplatsens ägare, eventuellt i samband med användarens aktivitet på webbplatsen, så att analytiska användningsrapporter kan genereras. De kan också genereras dynamiskt genom applikationslogik på klientsidan som tillhandahålls av enheten.

49. Spårningslänkar kan fungera på samma sätt, men identifieraren bifogas till webbplatsadressen. När användaren besöker URL:en (Uniform Resource Locator) laddar den berörda webbplatsen den begärda resursen, men samlar också in en identifierare som inte är relevant när det gäller resursidentifiering. Dessa används mycket ofta av e-handelswebbplatser för att identifiera ursprunget för deras inkommande trafik. Exempelvis kan sådana webbplatser tillhandahålla spårbara länkar till partner som

kan använda dem på sin domän så att e-handelswebbplatsen vet vilken av deras partner som är ansvarig för en försäljning och betalar en provision, en metod som kallas partnerprogram.

50. Både spårningslänkar och spårningspixlar kan distribueras via en mängd olika kanaler, t.ex. via e-post, webbplatser eller till och med, när det gäller spårningslänkar, via alla typer av textmeddelandesystem. Distributionen till användarens terminalutrustning utgör lagring, åtminstone genom den cachemekanism som finns i programvaran på klientsidan. Därmed är artikel 5.3 i direktivet om integritet och elektronisk kommunikation tillämplig, även om denna lagring inte är permanent.

51. Tillägg av spårningsinformation till URL eller bilder (pixlar) som skickas till användaren utgör en instruktion till terminalutrustningen om att skicka tillbaka den riktade informationen (den angivna identifieraren). När det gäller dynamiskt konstruerade spårningspixlar är det distributionen av den applikationslogiken (vanligtvis en JavaScript-kod) som utgör instruktionen. Som en följd av detta kan det anses att insamlingen av identifieringsuppgifter som tillhandahålls genom sådana spårningsmekanismer innebär att ”få tillgång” i den mening som avses i artikel 5.3 i direktivet om integritet och elektronisk kommunikation, och därför gäller det även för detta steg.

3.2 Lokal behandling

52. Vissa tekniker bygger på lokal behandling enligt instruktioner från programvara som distribueras på användarnas terminalutrustning, där den information som produceras av den lokala behandlingen sedan görs tillgänglig för utvalda aktörer via API på klientsidan. Detta kan till exempel vara fallet för ett API som tillhandahålls av webbläsaren, där lokalt genererade resultat kan nås på distans.

53. Om den behandlade informationen vid någon tidpunkt, t.ex. i koden på klientsidan, görs tillgänglig för en tredje part, t.ex. genom att den skickas tillbaka över nätverket till en server, skulle en sådan åtgärd (som instrueras av den enhet som producerar koden på klientsidan som distribueras på användarens terminalutrustning) vara att ”få tillgång till redan lagrad information”. Att denna information framställs lokalt utesluter inte tillämpning av artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

3.3 Spårning baserad endast på IP-adress

54. Vissa leverantörer utvecklar lösningar som endast förlitar sig på insamling av en komponent, nämligen IP-adressen, för att spåra användarens navigering[28], i vissa fall över flera domäner. I detta sammanhang skulle artikel 5.3 i direktivet om integritet och elektronisk kommunikation kunna vara tillämplig även om instruktionen att göra den aktuella IP-adressen tillgänglig har getts av en annan enhet än den mottagande.

55. Att få tillgång till IP-adresser skulle dock endast utlösa tillämpning av artikel 5.3 i direktivet om integritet och elektronisk kommunikation i fall där denna information härrör från en abonnents eller användares terminalutrustning. Även om det inte är systematiskt (t.ex. när CGNAT[29] är aktiverat), skulle statisk utgående IPv4 som kommer från en användares router omfattas av detta användningsfall, liksom IPV6-adresser eftersom de delvis definieras av värden. Såvida inte enheten kan säkerställa att

[28] Detta sker i tillägg till och oberoende av användningen och funktionen av en IP-adress för att upprätta och förmedla eller överföra av underliggande teknisk kommunikation, eller av att det kan vara eller inte vara personuppgifter (med avseende på analysen i direktivet om integritet och elektronisk kommunikation är det ”information”).

[29] Carrier-Grade NAT eller CGNAT används av internetleverantörer för att maximera användningen av begränsat IP-adressutrymme. Det grupperar ett antal abonnenter under samma offentliga IP-adress.

IP-adressen inte härrör från en användares eller abonnents terminalutrustning måste den vidta alla åtgärder i enlighet med artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

56. Även om dessa riktlinjer inte innefattar någon analys av tillämpningen av undantagen från skyldigheten att inhämta samtycke enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation, är det viktigt att än en gång påminna om att tillämpningen av denna artikel inte systematiskt innebär att samtycke måste inhämtas. EDPB påminner därför om att det i varje enskilt fall måste bedömas om ett samtycke krävs eller om ett undantag enligt artikel 5.3 i direktivet skulle kunna tillämpas[30].

3.4 Intermittent och förmedlad rapportering via sakernas internet

57. Enheter i sakernas internet (IoT-enheter, Internet of Things) producerar information kontinuerligt över tid, t.ex. genom sensorer som är inbäddade i enheten, som kan förbehandlas lokalt eller ej. I många fall görs information tillgänglig för en fjärrserver, men formerna för denna insamling kan variera.

58. Vissa IoT-enheter har en direkt anslutning till ett allmänt kommunikationsnät med ett mobilt SIM-kort. Andra kan ha en indirekt anslutning till ett allmänt kommunikationsnät, t.ex. genom användning av wifi eller överföring av information till en annan enhet genom en punkt-till-punkt-anslutning (t.ex. genom Bluetooth). Den andra enheten kan till exempel vara en smarttelefon eller en särskild nätsluss som eventuellt förbehandlar informationen innan den skickas till servern.

59. IoT-enheter kan instrueras av tillverkaren att alltid strömma den insamlade informationen, men ändå cachelagra informationen lokalt först, t.ex. tills en anslutning är tillgänglig.

60. I vilket fall som helst skulle IoT-enheten, när den är ansluten (direkt eller indirekt) till ett allmänt kommunikationsnät, i sig själv betraktas som en terminalutrustning. Att informationen strömmas eller cachas för intermittent rapportering ändrar inte informationens karaktär. I båda situationerna skulle artikel 5.3 i direktivet om integritet och elektronisk kommunikation vara tillämplig eftersom instruktionen från koden på IoT-enheten om att skicka de dynamiskt lagrade uppgifterna till fjärrservern, innebär att ”få tillgång”.

3.5 Unik identifierare

61. Ett vanligt verktyg som används av företag är begreppet ”unika identifierare” eller ”beständiga identifierare”. Sådana identifierare kan härledas från beständiga personuppgifter (för- och efternamn, e-post, telefonnummer etc.), som hashas på användarens enhet, samlas in och delas mellan flera personuppgiftsansvariga för att unikt identifiera en person i olika dataset (användningsdata som samlas in genom användning av webbplats eller applikation, kundhanteringsdata relaterade till köp eller prenumeration online eller offline etc.). På webbplatser inhämtas de beständiga personuppgifterna i allmänhet i samband med autentisering eller prenumeration på nyhetsbrev.

62. Såsom angetts ovan skulle det faktum att information förs in av användaren inte hindra tillämpningen av artikel 5.3 i direktivet om integritet och elektronisk kommunikation när det gäller lagring, eftersom denna information lagras tillfälligt på terminalutrustningen innan den samlas in.

63. När det gäller insamling av ”unika identifierare” på webbplatser eller i mobila applikationer instruerar den enhet som samlar in informationen webbläsaren (genom distribution av kod på klientsidan) att skicka den informationen. Därmed ges ”tillgång” och artikel 5.3 i direktivet om integritet och elektronisk kommunikation är tillämplig.

[30] I artikel 29-gruppens yttrande 9/2014 anges några exempel på när samtycke kanske inte behövs.