IMY. Integritetsskydds myndigheten

Platsbaserad och integritetsvänlig mobil direktkommunikation

Slutrapport från IMY:s innovationssandlåda för dataskydd

Diarienummer
IMY-2026-2532

Datum
2026-11-10



Om innovationssandlådan

IMY:s innovationssandlåda för dataskydd är en form av fördjupad vägledning där IMY, i nära dialog med deltagande aktörer, utforskar hur dataskyddsreglerna ska tolkas och tillämpas i praktiken. Syftet är att göra det enklare att utveckla innovativa och integritetssäkra tekniska lösningar.

I innovationssandlådan får offentliga och privata aktörer vägledning genom en serie workshops tillsammans med våra specialister inom juridik, teknik och informations- och cybersäkerhet. Vi prövar dataskyddsrättsliga frågor i tydligt avgränsade projekt, vilket ger oss möjlighet att analysera specifika utmaningar på djupet. Sandlådan innebär dock inte några undantag från dataskyddsreglerna. För att fler ska kunna ta del av projektens frågor, överväganden och slutsatser sammanfattas insikterna i en rapport.

Deltagare i innovationssandlådan väljs ut genom en öppen intresseanmälan, där projekt med samhällsnytta, innovationshöjd och behov av vägledning prioriteras. På så sätt bidrar innovationssandlådan till ökad kunskap om hur dataskydds-reglerna kan tillämpas i takt med den tekniska utvecklingen – och därmed till svensk innovation och konkurrenskraft.

Innehållsförteckning

Om innovationssandlådan 2
Ordlista 4
1. Sammanfattning 5
1.1. Platsbaserad mobil direktkommunikation 5
1.2. Slutsatser 5
2. Projektet 6
2.1. Bakgrund 6
2.2. Deltagaren 6
2.3. Målsättning 6
2.4. Tekniken 6
2.5. Dataskyddsfrågor 9
2.6. Avgränsningar och annan upplysning 9
3. Tokenisering som integritetsfrämjande teknik 10
3.1. Vad är anonyma och pseudonymiserade uppgifter? 10
3.2. Tokenisering i det aktuella projektet 10
3.3. Tokenisering begränsar informationsdelningen mellan aktörerna 11
3.4. Tokenisering som integritetsfrämjande teknik och rekommendationer för tjänstens utformning 11
3.5. IMY:s kommentar 13
4. Gränsdragningen mellan GDPR och e-dataskyddsdirektivet 14
4.1. Flera regelverk styr personuppgiftsbehandling 14
4.2. GDPR:s förhållande till e-dataskyddsdirektivet 14
4.3. E-dataskyddsdirektivets företräde 15
4.4. GDPR:s kompletterande roll 16
4.5. GDPR och e-dataskyddsdirektivet – när gäller vilket regelverk? 18
4.6. Individanpassad information till besökare 21
4.7. IMY:s kommentar 22
5. Fördelning av ansvar enligt GDPR 23
5.1. Ansvarsroller enligt GDPR 23
5.2. Scenario 1 – Inhämtning via mobilnätet 24
5.3. Scenario 2 – Inhämtning via GNSS-mottagare 24
5.4. Kommunikation med besökare och individanpassad information 25
5.5. IMY:s kommentar 26
6. Övriga reflektioner 27
7. Fördjupning 28

Ordlista

Deltagaren eller FastrMobi	FastrMobi AB, deltagaren i detta projekt i IMY:s innovationssandlåda
E-dataskyddsdirektivet	Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)
EDPB	Europeiska dataskyddsstyrelsen (eng. *European Data Protection Board*)
GDPR	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 (allmän dataskyddsförordning). ”GDPR” är en förkortning av det engelska namnet ”General Data Protection Regulation”
GNSS	Global Navigation Satellite System. Ett samlingsbegrepp för satellitbaserade system för positionsbestämning, exempelvis Galileo och GPS
IMY	Integritetsskyddsmyndigheten
LEK	Lagen (2022:482) om elektronisk kommunikation
MFL	Marknadsföringslagen (2008:486)
MSISDN	Mobile Station International Subscriber Directory Number. Ett unikt nummer som identifierar ett mobilabonnemang och som i praktiken motsvarar abonnentens mobiltelefonnummer
PTS	Post- och telestyrelsen
RCS	Rich Communication Services. En standard för meddelandetjänster som bland annat möjliggör interaktiva meddelanden
Tjänsten	Den tjänst för platsbaserad mobil direktkommunikation som analyseras i denna rapport
Tjänsteplattformen	FastrMobis tekniska plattform som hanterar de funktioner som behövs för tjänstens kommunikation, tokenhantering, matchning och samtyckeshantering

1. Sammanfattning

1.1. Platsbaserad mobil direktkommunikation

FastrMobi har utvecklat en lösning för platsbaserad mobil direktkommunikation som möjliggör kommunikation med personer via deras mobiler inom ett definierat geografiskt område. Rapporten utgår från hur tjänsten används i butiksmiljö, men de rättsliga frågorna kan aktualiseras även i andra sammanhang.

Rapporten behandlar två scenarier för att inhämta positioneringsuppgifter:

1. *Via mobilnätet – den lösning som FastrMobi har presenterat under projektet.*

2. *Via en GNSS-mottagare i användarens mobiltelefon.*

Det andra scenariot har tagits med för att tydliggöra hur den tekniska lösningen påverkar den rättsliga bedömningen.

Rapporten behandlar två huvudsakliga dataskyddsrättsliga frågor. Den första gäller hur GDPR och e-dataskyddsdirektivet förhåller sig till varandra vid de olika sätten att inhämta positioneringsuppgifter. Den andra handlar om hur personuppgiftsansvaret ska fördelas mellan de olika aktörerna som är involverade i användningen av tekniken. Aktörerna är i detta fall FastrMobi, mobiloperatören och butiken.

Rapporten behandlar även tokenisering som en integritetsfrämjande teknik. Genom att ersätta mobilnumret med en token kan aktörerna begränsa behovet av att dela direkt identifierande uppgifter. Om en tokeniserad uppgift är en personuppgift eller anonym information för en viss aktör beror bland annat på vilka ytterligare uppgifter och möjligheter till identifiering som aktören har.

1.2. Slutsatser

Hur ska gränsdragningen mellan GDPR och e-dataskyddsdirektivet göras i den aktuella behandlingen?

IMY bedömer att den teknik som används för att inhämta positioneringsuppgifter har betydelse för vilka regler som aktualiseras. Vid inhämtning via mobilnätet aktualiseras de särskilda reglerna om lokaliseringsuppgifter i e-dataskyddsdirektivet. Vid inhämtning genom åtkomst till information i användarens terminalutrustning, exempelvis via en GNSS-mottagare, kan i stället direktivets regler om lagring eller åtkomst till information i terminalutrustningen aktualiseras. GDPR gäller kompletterande i de frågor som inte regleras särskilt av e-dataskyddsdirektivet. Bedömningen behöver göras för varje behandlingsmoment med hänsyn till vilken teknik som används och vilka regler som är tillämpliga.

Vilka roller och ansvar enligt GDPR aktualiseras för de involverade aktörerna?

IMY bedömer att personuppgiftsansvaret ska bestämmas utifrån det konkreta behandlingsmomentet och vilka aktörer som bestämmer ändamål och väsentliga medel för behandlingen. De särskilda reglerna om positioneringsinhämtning behöver beaktas innan GDPR-rollerna för det momentet bedöms. För efterföljande behandlingar behöver rollerna bedömas separat. FastrMobi skapar token, kan koppla en identifierad kund till en specifik token och bestämmer hur länge kopplingen lagras. Detta talar starkt för att FastrMobi är personuppgiftsansvarig för dessa behandlingsmoment. För den fortsatta kommunikationen med besökare talar omständigheterna för att butiken är personuppgiftsansvarig för urval och utskick av individanpassad information, medan FastrMobis roll beror på hur bolaget medverkar i respektive behandling.

2. Projektet

2.1. Bakgrund

Platsbaserad mobil direktkommunikation innebär att information kan skickas direkt till en användares mobiltelefon när personen befinner sig inom ett definierat geografiskt område. Tekniken kan exempelvis användas för individanpassad service vid fysiska besök, såsom uppdateringar om ändrad gate på en flygplats, information om gångtid till en sjukhusavdelning, navigation och erbjudanden i en butik eller information vid en arena. FastrMobi har presenterat en patentsökt lösning som möjliggör sådan kommunikation utan att användarna behöver ladda ner en applikation eller ha tillgång till Wi-Fi.

I denna rapport används butiksmiljön som ett konkret exempel på användning av platsbaserad mobil direktkommunikation. För att belysa hur den tekniska lösningen påverkar de rättsliga förutsättningarna behandlas två scenarier för inhämtning av positioneringsuppgifter. Det första scenariot utgår från inhämtning via mobilnätet, i enlighet med den lösning som FastrMobi har presenterat under projektet. Det andra scenariot, som har inkluderats av IMY inom ramen för rapporten, utgår från inhämtning via en GNSS-mottagare i användarens mobiltelefon.

Genom att belysa båda scenarierna kan rapporten tydliggöra hur valet av teknik påverkar den rättsliga bedömningen och ge vägledning som även kan vara relevant för andra tekniska lösningar och användningsområden.

Vägledningen i projektet har fokuserat på två rättsliga frågeställningar. Därutöver har projektet berört tokenisering som en integritetsfrämjande teknik, bland annat utifrån dess betydelse för hanteringen och skyddet av personuppgifter inom tjänsten.

Utöver de frågor som har behandlats inom projektet finns andra juridiska frågor som behöver beaktas innan en tjänst motsvarande den aktuella kan driftsättas. Dessa frågor har inte analyserats inom ramen för projektet.

2.2. Deltagaren

FastrMobi är ett företag som utvecklar lösningar för mobil direktkommunikation och platsbaserade mobiltjänster. Bolaget arbetar bland annat med patentsökt teknik för geografiskt anpassad kommunikation via mobilnät och utvecklar tjänster som möjliggör riktade informationsutskick till mobiltelefoner inom definierade områden.

2.3. Målsättning

FastrMobi har presenterat ett projekt med användning av platsbaserad mobil direktkommunikation i butiksmiljö. Projektet går ut på att FastrMobis tjänst ska användas för geografiskt anpassade informationsutskick till mobiltelefoner inom ett visst område för att kunna kommunicera med personer som befinner sig där. Det är alltså detta användningsfall som rapporten baseras på. Platsbaserad mobil direktkommunikation kan dock användas i flera olika miljöer och för många andra ändamål. De rättsliga frågor som behandlas i denna rapport kan därför vara relevanta även vid andra användningsområden.

Målet med sandlådeprojektet har varit att analysera gränsdragningen mellan de regelverk som blir aktuella vid behandlingen av personuppgifter i tjänsten och hur det dataskyddsrättsliga ansvaret är fördelat mellan involverade aktörer.

2.4. Tekniken

Övergripande arkitektur och aktörer
Tjänsten bygger på en teknisk kedja där flera aktörer och systemkomponenter ingår och som, tillsammans med mobilnätet, används för att detektera när en kund befinner sig i

ett anslutet område. När kunden detekteras skickas mobilnumret (MSISDN) till FastrMobi, där det ersätts med en unik token innan uppgiften förs vidare i tjänstekedjan. Den fortsatta kommunikationen sker genom FastrMobis tjänsteplattform. Om kunden har valt en funktion i plattformen som medger identifiering, kan en token därefter matchas mot en registrerad kundprofil innan relevant information görs tillgänglig för butiken.

Plattformen kan även lagra och hantera uppgifter som behövs för samtycke och för att styra kommunikationen med kunden. Kunden och butiken kan interagera med tjänsten genom de gränssnitt som ingår i plattformen. Butiken kan även integrera tjänsten med egna system, exempelvis CRM-, webb- och meddelandesystem.

Tokeniseringens närmare utformning och betydelse beskrivs i avsnitt 3 nedan.

Detektering och kommunikation med kunden
När en kund kommer in i en butik som är utrustad med en lokalt installerad basstation, kan kundens mobiltelefon ansluta till basstationen på samma sätt som vid annan kommunikation i mobilnätet. I den aktuella lösningen används denna nätfunktionalitet även för att detektera att kunden befinner sig inom det område där tjänsten tillhandahålls. Därefter förs den information som behövs för tjänsten vidare i den tekniska kedjan.

Som en del av denna process skapas en unik och slumpmässig token som används under den fortsatta kommunikationen. Därmed undviks användning av mobilnumret (MSISDN). Den fortsatta kommunikationen kan därefter hanteras genom FastrMobis plattform och RCS.[1]

FastrMobis tjänsteplattform
FastrMobis tjänsteplattform fungerar som ett tekniskt lager mellan mobilnätet, butiken och kommunikationslösningen. Plattformen hanterar bland annat tokeniserade identifierare och kan, när förutsättningarna är uppfyllda, matcha en token mot en registrerad kundprofil.

Den närmare tekniska utformningen av tokeniseringen, inklusive vilka identifierare som används och hur informationen fördelas mellan mobiloperatören, FastrMobi och butiken, behandlas i avsnitt 3 nedan.

Avgränsning av vilka kunder som omfattas av tjänsten
Ytterligare en del av den tekniska arkitekturen är möjligheten att begränsa vilka kunder som över huvud taget omfattas av tjänsten. Av det projektmaterial som IMY har tagit del av framgår att lösningen bygger på en modell där en mobiloperatör har kontroll över vilka kunder som detekteras och där tjänsten bygger på att kunden har lämnat sitt samtycke till att bli positionerade och behandlade för tjänstens funktionalitet.

I moderna mobilnät finns tekniska möjligheter att styra vilka användare eller enheter som får tillgång till en viss nätverksfunktion eller tjänst. Detta uppnås genom abonnemangsbaserad tilldelning av nätverksresurser. Detta är en form av virtualisering där en separering av nätverkets fysiska och logiska funktioner gör det möjligt att tilldela specifika resurser och behörigheter till en viss användargrupp – i detta fall de kunder som har tecknat abonnemang med mobiloperatören och samtyckt till att FastrMobis tjänst ingår som en del av abonnemanget.

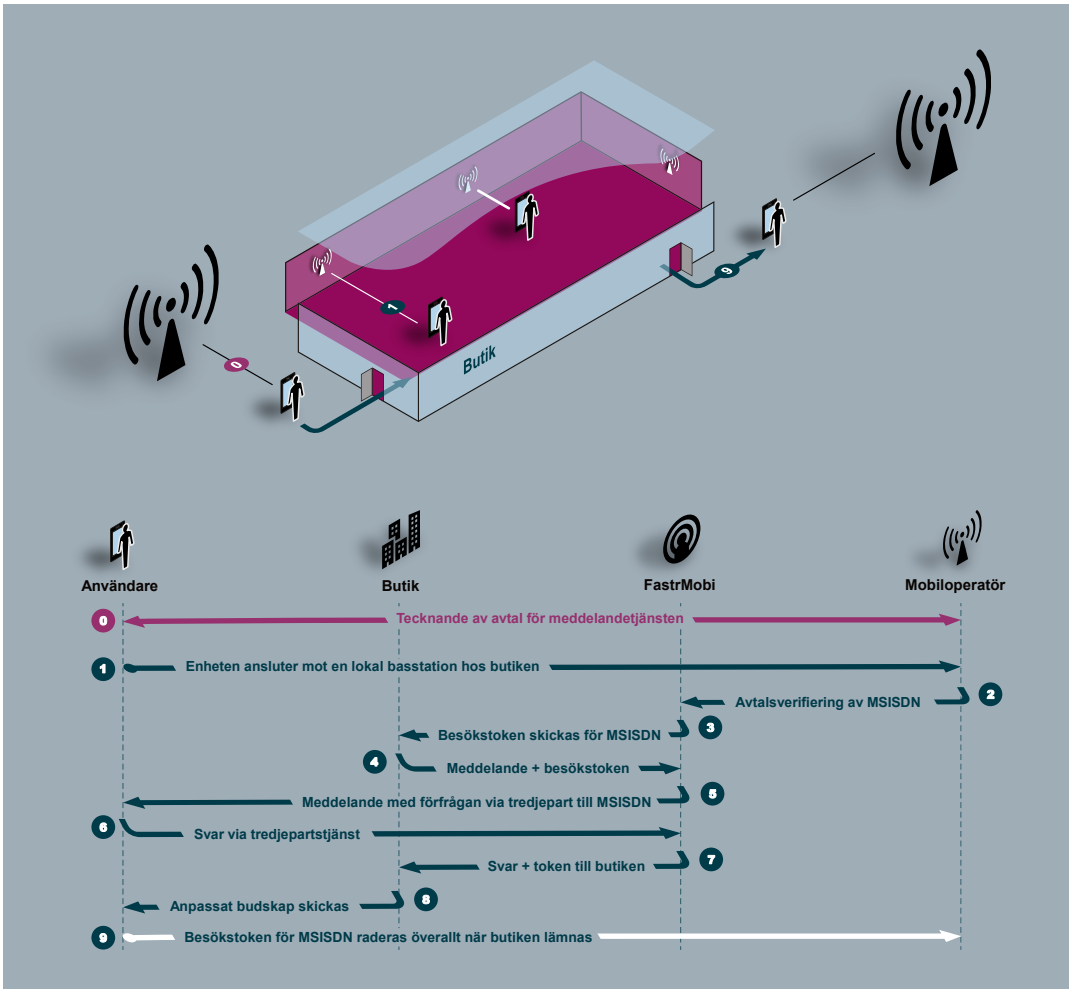
[1] RCS (Rich Communication Services) är en standard för meddelandetjänster som möjliggör utökade funktioner jämfört med traditionella SMS, såsom interaktiva meddelanden. I den aktuella tjänsten används RCS för att kunden ska kunna ta emot information och göra val som styr den fortsatta kommunikationen med butiken.

För den aktuella tjänsten innebär detta att det tekniskt kan finnas möjligheter att utforma mobilnätsdelen så att endast kunder som omfattas av tjänsten kan detekteras eller behandlas inom den aktuella tjänstefunktionen.

Den tekniska avgränsningen är en central förutsättning för den fortsatta analysen eftersom det behöver säkerställas att endast kunder som omfattas av tjänsten detekteras eller behandlas inom den aktuella tjänstefunktionen. De rättsliga förutsättningarna för behandlingen av personuppgifter i tjänsten för direktmarknadsföring behandlas i avsnitt 4 nedan.

För att belysa hur valet av teknik för närvarodetektering påverkar den rättsliga bedömningen behandlas även ett alternativt scenario där närvarodetektering sker genom GNSS-positionering via en applikation. I detta scenario hanteras samtycket och datainsamlingen direkt i användarens enhet i stället för via nätverksinfrastrukturen.

Sammanfattningsvis är avsikten att tjänsten ska fungera enligt följande.



0. Användaren tecknar ett avtal för meddelandetjänsten med mobiloperatören.
1. Enheten kopplas upp mot en lokal basstation när en användare kommer in i en butik (eller annan verksamhet) som är ansluten. Enheten identifieras som tillhörande den särskilda nätverksresursen på basstationsnivå. Endast kunder som tillhör denna nätverksresurs behandlas i resterande steg.
2. FastrMobi får information av mobiloperatören om att ett avtalsverifierat MSISDN anslutit till en basstation i butiken.
3. En unik besökstoken kopplad till den specifika butiken skapas för det anslutna MSISDN:et.
4. Butiken skickar ett meddelande samt besökstoken till FastrMobi.

5. Meddelandet skickas till användaren. Användaren får välja om denne vid besöket vill kopplas mot en kundprofil eller ej.
6. Användaren meddelar sina preferenser för besöket.
7. FastrMobi meddelar butiken om användarens önskan om att vara kopplad mot sin kundprofil eller ej.
8. Butiken skickar meddelande till användaren om erbjudanden eller annan typ av information.
9. Besökstoken kopplad till MSISDN raderas när användaren lämnar butiken. Detta gäller i alla led för samtliga aktörer.

2.5. Dataskyddsfrågor

FastrMobi enades tillsammans med IMY om att fokusera på följande övergripande dataskyddsfrågor i det aktuella projektet:

- **Hur ska gränsdragningen mellan GDPR och e-dataskyddsdirektivet göras i den aktuella behandlingen?**
- **Vilka roller och ansvar enligt GDPR aktualiseras för de involverade aktörerna?**

2.6. Avgränsningar och annan upplysning

Denna rapport fokuserar på två rättsfrågor som har identifierats som relevanta för deltagaren. Det bör noteras att den aktuella tjänsten ännu inte är driftsatt och att ytterligare juridiska och tekniska aspekter som IMY inte behandlar i rapporten behöver utredas av deltagaren innan tjänsten tas i drift.

Utifrån den arkitektur som analyseras i rapporten är det en central förutsättning att mobilnätsdelen tekniskt avgränsas så att endast kunder som omfattas av tjänsten detekteras eller behandlas inom den aktuella tjänstefunktionen. Om en sådan avgränsning inte kan genomföras behöver den tekniska lösningen och de rättsliga förutsättningarna bedömas på nytt.

Eftersom behandlingen hos deltagaren och den avtalade leverantören ska ske inom Sverige och EU har frågor kring dataöverföring till tredjeland inte analyserats.[2]

Denna rapport redogör för IMY:s uppfattning i dataskyddsrättsliga frågor där det finns behov av vägledning. Bedömningarna görs mot bakgrund av nuvarande rättsläge och kan komma att ändras om det skulle komma ny lagstiftning, domstolspraxis eller vägledning från EDPB[3].

Inom ramen för detta projekt har IMY haft kontakt med PTS och Konsumentverket med anledning av de delar av rapporten som berör deras respektive tillsynsområden.

[2] Mer information om så kallade tredjelandsfrågor finns på IMY:s webbplats (https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land).
[3] Läs mer om EDPB på IMY:s webbplats (https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-eu-niva/edbp/).

3. Tokenisering som integritetsfrämjande teknik

Tokenisering är en form av pseudonymisering och kan användas som en integritetsfrämjande teknik för att minska behovet av att dela direkt identifierande uppgifter mellan aktörer.[4] Genom att ersätta en identifierande uppgift, i det här fallet ett mobilnummer, med en unik sträng av slumpmässiga nummer (så kallad token), kan tjänsten utformas så att aktörer som inte behöver känna till den ursprungliga identifieraren i stället hanterar tokeniserade uppgifter. Teknikens integritetsfrämjande effekt beror på hur tokeniseringen kombineras med informationsseparation, åtkomstbegränsningar och andra tekniska och organisatoriska skyddsåtgärder.[5]

3.1. Vad är anonyma och pseudonymiserade uppgifter?

En uppgift är anonym för en aktör om den registrerade, det vill säga en fysisk person, inte längre kan identifieras med de medel som rimligen kan användas i det aktuella sammanhanget. Bedömningen är beroende av bland annat vilken ytterligare information aktören har tillgång till och vilka möjligheter som finns att kombinera uppgifter. Detta är relevant för tokenisering eftersom en token kan kraftigt begränsa möjligheten att informationen kopplas till en direkt identifierare utan att detta i sig avgör om uppgiften är anonym.[6]

Pseudonymiserade personuppgifter är fortfarande personuppgifter, men kan minska riskerna för de registrerade och användas som en teknisk och organisatorisk skyddsåtgärd. [7] För den aktuella tjänsten är detta relevant eftersom tokenisering gör det möjligt att separera den direkt identifierande uppgiften från den information som behövs för tjänstens fortsatta funktion.

3.2. Tokenisering i det aktuella projektet

I den tilltänkta tjänsten används token för att minska behovet av att dela identifierande uppgifter mellan de aktörer som deltar i tjänsten. Ett mobilnummer ersätts med en unik token som används i den fortsatta kommunikationen mellan aktörerna.

Tokeniseringen sker genom att FastrMobi ersätter mobilnumret med en unik token. Därefter kan FastrMobis tjänsteplattform, när förutsättningarna är uppfyllda, använda ytterligare information för att matcha token mot en registrerad kundprofil. Tokeniseringen och den efterföljande matchningen är således två olika tekniska funktioner i tjänstens arkitektur.

Tillgång till identifierare och koppling till fysisk person
Informationsfördelningen mellan aktörerna innebär att varje aktör får tillgång till de delar av informationen som behövs för att aktören ska kunna fullgöra sin roll i tjänsten. Mobiloperatören hanterar mobilnumret i mobilnätet. FastrMobi hanterar huvudsakligen token och kan matcha en token mot en registrerad kundprofil. Butiken får genom tjänsten tillgång till den information som behövs för den fortsatta kommunikationen med kunden utan att mobilnumret behöver exponeras.

---

[4] Pseudonymisering är en etablerad integritetsfrämjande teknik. Se *En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning*, SOU 2026:44.
[5] Integritetsfrämjande tekniker (eng. *Privacy Enhancing Technologies, PET*) är ett samlingsbegrepp för tekniska lösningar som är utformade för att skydda individers personliga integritet. Se Integritetsskyddsmyndigheten, *Betrodda exekveringsmiljöer för uppkopplade fordon*, avsnitt 2.5, s. 8.
[6] EDPB, *Guidelines 02/2026 on Anonymisation*, version 1.0. Riktlinjerna antogs för offentligt samråd den 7 juli 2026 och är ännu inte slutligt antagna. För att data ska anses anonyma behöver samtliga kriterier som riktlinjerna ställer upp uppfyllas. Se vidare s. 16 ff. för den tekniska analysen av anonymisering.
[7] EDPB, *Guidelines 01/2025 on Pseudonymisation*. Riktlinjerna antogs för offentligt samråd den 16 januari 2025 och är ännu inte slutligt antagna.

3.3. Tokenisering begränsar informationsdelningen mellan aktörerna

I den aktuella tjänsten sker tokeniseringen hos FastrMobi. När en kund detekteras i mobiloperatörens nät kontrollerar mobiloperatören om kundens abonnemang har tillägget för meddelandetjänsten. Om så är fallet kan kundens mobilnummer överföras till FastrMobi, som då kan ersätta mobilnumret med en unik token. Denna token används därefter som identifierare i den fortsatta kommunikationen mellan FastrMobi och butiken för att möjliggöra meddelanden till kunden.

FastrMobis tjänsteplattform hanterar därefter token och de funktioner som krävs för den fortsatta kommunikationen. Om kunden i förväg har registrerat sitt mobilnummer och lämnat det samtycke som krävs, kan tjänsteplattformen även använda ytterligare information för att koppla mobilnumrets token till en registrerad kundprofil. Denna matchning gör det möjligt att tillhandahålla funktioner som kräver en koppling till en kundprofil utan att mobilnumret behöver lämnas ut till butiken. Butiken kan därmed kommunicera med kunden utan att få tillgång till den direkt identifierande uppgiften, det vill säga mobilnumret. Kommunikationen sker i stället med hjälp av den token och den information som tjänsten gör tillgänglig.

Informationsseparationen kan illustreras genom att skilja mellan tre typer av information:

- **Direkt identifierande information** som hanteras inom mobiloperatörens miljö, exempelvis mobilnumret.

- **Identifierande token**, det vill säga den token som används för att möjliggöra den fortsatta kommunikationen mellan aktörerna utan att mobilnumret behöver delas.

- **Kundprofil**, det vill säga uppgifter om en registrerad kund som kan användas för att tillhandahålla individanpassade funktioner. Uppgifterna kan kopplas till kundens token när förutsättningarna för matchning är uppfyllda.

Hur denna tekniska informationsseparation påverkar bedömningen av om token utgör personuppgifter eller anonyma uppgifter beror på vilka uppgifter respektive aktör har tillgång till och vilka möjligheter aktören har att koppla uppgifterna till en fysisk person. Tokeniseringens funktion som integritetsfrämjande teknik består därför framför allt i att minska exponeringen av direkt identifierande uppgifter och att begränsa informationsdelningen mellan aktörerna.

Det är också viktigt att skilja mellan **informationsseparation** och **anonymisering**. Att en aktör inte får tillgång till mobilnumret innebär inte i sig att de tokeniserade uppgifterna är anonyma. Tokeniseringen kan däremot bidra till att minska mängden information som behöver göras tillgänglig för respektive aktör och därmed minska risken för att uppgifter kopplas samman på ett sätt som inte behövs för tjänstens funktion. Detta är en central del av hur tokenisering kan användas som en integritetsfrämjande teknik.

3.4. Tokenisering som integritetsfrämjande teknik och rekommendationer för tjänstens utformning

Den primära integritetsfrämjande effekten av tokenisering kommer av den pseudonymisering av direkt identifierande uppgifter som sker. För att denna effekt ska bestå i praktiken behöver tokeniseringen kombineras med åtkomstbegränsningar, informationsseparation, kontrollerad matchning, begränsad lagringstid och tydlig styrning av användarens val.

1. Förstärkt användarkontroll och samtyckeshantering
Systemet bör utformas så att användaren har kontroll över sin synlighet och över hur personuppgifter används inom tjänsten. Det kan exempelvis ske genom följande åtgärder.

- **Flexibelt återkallande av samtycke**
  Det bör finnas en funktion som gör det enkelt för användaren att kunna återkalla sitt samtycke, exempelvis för en specifik butik eller för tjänsten som helhet. Vid ett återkallande bör kopplingar mellan mobilnummer, token och kundprofiler raderas eller göras ogiltiga i den utsträckning uppgifterna inte längre behöver behandlas för något annat ändamål.

- **Dynamisk statusstyrning**
  Systemet bör vara utformat så att kunden vid varje enskilt besök ges möjlighet att välja hur kommunikationen med butiken ska ske, exempelvis utan koppling till kundprofil respektive med koppling till kundprofil. Ett tidigare val bör inte låsa användaren i en identifierad status, utan användaren bör kunna göra ett aktivt val vid varje interaktion.

- **Tydlig transparens via RCS**
  Kommunikationen via RCS bör utformas så att kunden tydligt informeras om vad ett val innebär vid den aktuella interaktionen och hur kunden enkelt kan ändra sitt val eller återgå till att inte längre vara kopplad mot en kundprofil.

2. Tekniska krav på datasäkerhet och isolering
För att minimera risken för dataläckage och obehörig identifiering bör bland annat följande säkerhetsmekanismer integreras i arkitekturen.

- **Strikt isolering av dataflöden**
  Systemet bör utformas med en strikt teknisk separation mellan dataflöden för kunder som har valt att inte vara kopplade till en kundprofil och kunder som har valt att vara det. API-anrop och databasanrop bör utformas så att butiken inte kan få tillgång till uppgifter i den registrerade kundprofil som hanteras av FastrMobi eller andra identifierande uppgifter som inte är nödvändiga för tjänstens funktion.

- **Kryptering och skydd av identifierande information**
  Information som lagras i tjänsteplattformen bör skyddas med lämpliga tekniska och organisatoriska säkerhetsåtgärder. Om mobilnummer behöver lagras bör det bedömas om uppgifterna kan ersättas eller skyddas genom en annan teknisk lösning utifrån den funktionalitet som krävs och de identifierade riskerna.

- **Automatiserad livscykelhantering av data**
  Det bör implementeras strikta rutiner för dataminimering där närvarodata och temporära tokens raderas eller görs obrukbara efter en definierad tidsperiod. Detta minskar risken för att historiska data kan användas för att kartlägga individers rörelsemönster över tid.

3. Kontrollmekanismer och spårbarhet
För att säkerställa att integritetsskyddet upprätthålls i praktiken bör systemet innehålla funktioner för granskning och verifiering. Nedan följer exempel på sådana åtgärder.

- **Implementering av skyddade säkerhetsloggar**
  Anrop till tjänsteplattformens matchningsfunktion som syftar till att koppla en token till en kundprofil bör loggas på ett sätt som möjliggör efterhandskontroll och oberoende granskning av att identifiering endast sker när förutsättningarna för detta är uppfyllda.

- **Verifiering av samtyckeskedjan**
  Innan identifierande information överförs från FastrMobi till butiken bör systemet automatiskt kontrollera att det finns ett aktuellt och giltigt stöd för den aktuella behandlingen och att överföringen motsvarar kundens aktuella val.

3.5. IMY:s kommentar

Tokenisering är en integritetsfrämjande teknik genom att direkt identifierande uppgifter ersätts med token och därmed inte behöver exponeras för alla aktörer som deltar i en tjänst. I den aktuella arkitekturen innebär detta bland annat att mobilnumret kan ersättas med en token innan informationen förs vidare i tjänstekedjan. Tekniken kan därigenom bidra till att begränsa spridningen av identifierande uppgifter och minska mängden information som olika aktörer behöver ha tillgång till och behandla. Den integritetsfrämjande effekten förstärks när tokenisering kombineras med informationsseparation, åtkomstbegränsningar, kontrollerad matchning, begränsad lagring och möjlighet för användaren att styra hur informationen används.

Tokenisering bör därmed inte betraktas som ett självständigt integritetsskydd, utan som en del av en bredare teknisk och organisatorisk utformning. Den integritetsfrämjande effekten beror bland annat på hur kopplingen mellan token och identifierande uppgifter skyddas, vilka aktörer som har tillgång till ytterligare information, hur länge uppgifter sparas och vilka möjligheter som finns att koppla samman uppgifter från olika källor.

4. Gränsdragningen mellan GDPR och e-dataskyddsdirektivet

4.1. Flera regelverk styr personuppgiftsbehandling

Digitala tjänster, som de tjänster FastrMobi utvecklar, kan innebära behandling av personuppgifter genom att användares geografiska position inhämtas samt genom kommunikation och direktmarknadsföring till användare.[8] GDPR är det generella regelverket för behandling av personuppgifter. E-dataskyddsdirektivet är en specialreglering som innehåller bestämmelser som kompletterar GDPR och preciserar kraven inom området elektronisk kommunikation. Vissa bestämmelser gäller även information som inte utgör personuppgifter.

För verksamheter som hanterar personuppgifter inom elektronisk kommunikation kan det vara utmanande att avgöra vilka krav som gäller och hur olika regelverk förhåller sig till varandra. Både GDPR och e-dataskyddsdirektivet är tillämpliga vid behandling av personuppgifter inom området för elektronisk kommunikation. Detta aktualiserar behovet av att klargöra hur man avgör vilket regelverk som gäller i varje given situation.

Gränsdragningen mellan GDPR och e-dataskyddsdirektivet är inte alltid självklar då regelverkens tillämpningsområde delvis är överlappande. En god förståelse för hur regelverken samverkar är avgörande för att säkerställa rättslig efterlevnad, undvika onödiga överlappningar och minimera riskerna för brister i dataskyddet.

GDPR är en EU-förordning som är direkt tillämplig i alla EU-länder. E-dataskyddsdirektivet är däremot ett EU-direktiv som medlemsstaterna införlivar i nationell lagstiftning. Avsnittet utgår från e-dataskyddsdirektivet men när hänvisning görs till skyldigheter som har sin grund i direktivets artiklar anges var dessa har genomförts i svensk rätt.

Genomförandet av ett direktiv innebär emellertid inte att varje direktivbestämmelse måste ha en uttrycklig motsvarighet i nationell lagstiftning. Beroende på bestämmelsens innehåll kan direktivets krav säkerställas utan att bestämmelsen återges särskilt i svensk rätt. Detta gäller exempelvis bestämmelser som anger direktivets syfte eller systematiska förhållande till annan EU-rätt.

I Sverige har e-dataskyddsdirektivet genomförts i LEK och MFL, vilka utgör den svenska regleringen som är direkt tillämplig på berörda aktörer. I Sverige är IMY tillsynsmyndighet för GDPR, PTS är tillsynsmyndighet för LEK och Konsumentverket är tillsynsmyndighet för MFL.

Avsnittet berör således flera olika regelverk som lyder under olika tillsynsmyndigheter. Fokus ligger på gränsdragningen mellan regelverken utifrån ett GDPR-perspektiv och inom ramen för IMY:s ansvarsområde.[9]

4.2. GDPR:s förhållande till e-dataskyddsdirektivet

GDPR innehåller bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter, enligt artikel 1 GDPR. GDPR är det generella regelverket för behandling av personuppgifter och är teknikneutral, med de avgränsningar som följer av förordningens tillämpningsområde. Det innebär att när en verksamhet behandlar personuppgifter ska GDPR:s allmänna

[8] Artiklarna 2 c, 5 och 13 e-dataskyddsdirektivet.
[9] För närmare vägledning om tillämpningen och tolkningen av LEK respektive MFL hänvisas till PTS respektive Konsumentverket.

bestämmelser om personuppgiftsbehandling tillämpas i den mån inte särskilda regler i e-dataskyddsdirektivet gäller för det aktuella behandlingsmomentet.

Vid sidan av GDPR:s allmänna bestämmelser om personuppgiftsbehandling finns särskilda bestämmelser i kompletterande lagstiftning. Inom området för elektronisk kommunikation kompletteras GDPR av e-dataskyddsdirektivet, som innehåller bestämmelser om bland annat integritet och konfidentialitet vid elektronisk kommunikation. Enligt artikel 1 e-dataskyddsdirektivet preciserar och kompletterar direktivet det tidigare dataskyddsdirektivet. Hänvisningarna till det direktivet ska enligt artikel 94.2 GDPR läsas som hänvisningar till GDPR.

E-dataskyddsdirektivet innehåller bestämmelser som riktar sig till olika aktörer beroende på vilken typ av verksamhet de bedriver och i vilket syfte de behandlar uppgifter. Det finns bestämmelser som endast gäller tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster eller -nät. Andra bestämmelser i direktivet har ett bredare tillämpningsområde och gäller alla som lagrar eller får tillgång till information i en användares terminalutrustning, till exempel en webbplatsoperatör. Det finns även bestämmelser om elektronisk direktmarknadsföring som inte är begränsade till tillhandahållare av elektroniska kommunikationstjänster.

E-dataskyddsdirektivet innehåller bland annat bestämmelser som anger under vilka förutsättningar uppgifter får behandlas och hur uppgifter ska skyddas mot till exempel obehörig åtkomst.[10]

4.3. E-dataskyddsdirektivets företräde

Artikel 95 och skäl 173 GDPR behandlar förordningens förhållande till e-dataskyddsdirektivet. För behandling av personuppgifter i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät medför GDPR inte ytterligare skyldigheter i den mån direktivet redan föreskriver särskilda skyldigheter för samma ändamål. GDPR gäller däremot i frågor som direktivet inte reglerar särskilt, bland annat i fråga om den personuppgiftsansvariges skyldigheter och fysiska personers rättigheter. Samma förhållande till GDPR kommer till uttryck i skäl 10 e-dataskyddsdirektivet. Det innebär att e-dataskyddsdirektivets särskilda regler har företräde i de frågor som de reglerar, medan GDPR gäller kompletterande i övriga delar.

Det handlar därför inte om ett val mellan två regelverk utan snarare om två regelverk som ska tillämpas parallellt men där en stegvis bedömning behöver ske eftersom vissa materiella krav i e-dataskyddsdirektivet har företräde framför andra i GDPR. Först fastställs om e-dataskyddsdirektivet är tillämpligt och reglerar en viss fråga. Därefter används GDPR som komplettering. Bedömningen behöver alltså göras för den aktuella behandlingen och den särskilda skyldighet som är i fråga.

I en dom från EU-domstolen (den så kallade Inteligo-domen)[11] illustreras hur gränsdragningen mellan e-dataskyddsdirektivet och GDPR ska göras. Målet gällde bland annat om villkoren för laglig behandling i artikel 6.1 GDPR ska tillämpas parallellt med artikel 13.2 e-dataskyddsdirektivet, som reglerar viss direkt marknadsföring och har genomförts i svensk rätt genom 19 § andra stycket MFL. EU-domstolen konstaterade att artikel 13.2 uttömmande reglerar villkoren och ändamålen för den aktuella behandlingen samt den registrerades rättigheter. Bestämmelsen innebär därmed sådana särskilda skyldigheter som avses i artikel 95 GDPR. När en personuppgiftsansvarig använder en användares e-postadress för att skicka kommunikation i enlighet med artikel 13.2 ska lagligheten därför bedömas utifrån den bestämmelsen, utan någon parallell prövning enligt artikel 6.1 GDPR. GDPR är däremot

[10] Jfr artiklarna 4.1, 5 och 6 e-dataskyddsdirektivet.
[11] EU-domstolens dom den 13 november 2025, Inteligo Media, C-654/23, EU:C:2025:871.

fortsatt tillämplig på frågor som inte omfattas av särskilda skyldigheter med samma syfte enligt e-dataskyddsdirektivet.[12]

4.4. GDPR:s kompletterande roll

GDPR är, inom sitt tillämpningsområde, tillämplig på elektronisk kommunikation i de frågor som inte regleras särskilt i e-dataskyddsdirektivet. Enligt artikel 2 e-dataskyddsdirektivet, läst tillsammans med artikel 94.2 GDPR, ska dessutom vissa av GDPR:s definitioner gälla när e-dataskyddsdirektivet tillämpas.

Ett exempel på en sådan situation är regleringen av samtycke. Medan e-dataskyddsdirektivet fastställer i vilka situationer samtycke krävs, hänvisar det för själva definitionen av ett giltigt samtycke till GDPR. När e-dataskyddsdirektivet uppställer krav på samtycke är det GDPR som anger vad som krävs för att samtycket ska vara giltigt. Definitionen av samtycke i artikel 4.11 och villkoren i artikel 7 GDPR gäller därför även vid tillämpningen av e-dataskyddsdirektivets bestämmelser. E-dataskyddsdirektivet kan således innehålla den särskilda regeln om när samtycke krävs för en viss behandling, medan GDPR anger de materiella kraven för samtyckets giltighet. När deras respektive tillämpningsförutsättningar är uppfyllda behöver även de särskilda kraven i artiklarna 8 och 9.2 a GDPR beaktas.

Samtycke definieras i artikel 4.11 GDPR som en frivillig, specifik, informerad och otvetydig viljeyttring genom vilken den registrerade, genom ett uttalande eller en entydig bekräftande handling, godtar behandling av personuppgifter som rör denne.

Att samtycket ska vara *frivilligt* innebär att den registrerade ska ha en genuin valmöjlighet och faktisk kontroll över behandlingen. Samtycket är inte frivilligt om den registrerade känner sig tvingad att samtycka eller riskerar nackdelar som i praktiken begränsar möjligheten att vägra eller återkalla samtycket.[13]

Att samtycket ska vara *specifikt* innebär att det ska avse ett eller flera tydligt angivna ändamål. Ändamålet med behandlingen behöver därför fastställas innan samtycke begärs. Vagt eller allmänt formulerade ändamål som inte gör det möjligt för den registrerade att förstå vad uppgifterna ska användas till uppfyller normalt inte kravet på ett specifikt samtycke.[14] Om personuppgifterna ska behandlas för flera skilda ändamål ska den registrerade som utgångspunkt kunna ta ställning till varje ändamål separat.[15]

Att samtycket ska vara *informerat* innebär att den registrerade ska kunna fatta ett informerat beslut. Innan samtycket lämnas ska den registrerade få tillräcklig information för att förstå vilken behandling som godtas och vilka följder samtycket kan få.[16]

Informerat samtycke kräver att den registrerade åtminstone får information om

- den personuppgiftsansvariges identitet,
- ändamålet med varje behandling som samtycke begärs för,
- vilka personuppgifter eller kategorier av personuppgifter som ska samlas in och användas,
- rätten att återkalla samtycket,

[12] EU:C: 2025:871, punkterna 64–69.
[13] EDPB:s riktlinjer 05/2020 om samtycke enligt förordning 2016/679, version 1.1, s. 8, p. 13 samt s. 13, p. 46–49.
[14] EDPB:s riktlinjer 05/2020, s. 14–15, p. 55–57.
[15] EDPB:s riktlinjer 05/2020, s. 15, p. 58–61.
[16] EDPB:s riktlinjer 05/2020, s. 15, p. 62.

- förekomsten av automatiserat beslutsfattande enligt artikel 22.2 c GDPR, om sådan behandling förekommer, och

- eventuella risker med överföring av personuppgifter till tredjeland i avsaknad av beslut om adekvat skyddsnivå och lämpliga skyddsåtgärder, om överföringen ska stödjas på uttryckligt samtycke enligt artikel 49.1 a GDPR.[17]

Vilken information som behöver lämnas kan variera beroende på behandlingens sammanhang och komplexitet. Om flera personuppgiftsansvariga avser att stödja sin behandling på samma samtycke, ska samtliga dessa organisationer anges med namn. Det är alltså normalt inte tillräckligt att endast ange att uppgifterna får lämnas till eller behandlas av exempelvis ”samarbetspartner” eller ”tredje parter”.[18]

Att samtycket ska utgöra en *otvetydig viljeyttring* innebär att den registrerade genom ett uttalande eller en entydig bekräftande handling aktivt ska visa att den aktuella behandlingen godtas. Det ska vara möjligt att objektivt fastställa att den registrerades agerande avsåg ett godkännande av just den behandling som samtyckesbegäran omfattade.[19]

Artikel 7 GDPR anger vidare de villkor som gäller för ett giltigt samtycke.

Ett samtycke kan lämnas i en skriftlig förklaring som även rör andra frågor, exempelvis i samband med att ett avtal ingås. Ett godkännande av avtalet eller de allmänna villkoren innebär dock inte i sig att den registrerade har samtyckt till behandling av personuppgifter. Samtyckesbegäran måste i sådana fall presenteras på ett sätt som klart och tydligt kan särskiljas från övriga avtalsvillkor samt vara begriplig och lättillgänglig.[20]

Samtycket ska inhämtas innan den behandling som kräver samtycke påbörjas.[21] För behandling av särskilda kategorier av personuppgifter med stöd av artikel 9.2 a GDPR krävs att samtycket är uttryckligt. Kravet avser hur den registrerade ger uttryck för sitt samtycke och innebär ett högre krav på tydlighet och bevisning. Uttryckligt samtycke kan exempelvis lämnas genom en undertecknad förklaring, en elektronisk signatur eller en dokumenterad muntlig bekräftelse som klart avser den aktuella behandlingen.[22]

GDPR kräver inte att den personuppgiftsansvarige själv rent praktiskt inhämtar samtycket. Samtycket kan exempelvis inhämtas av en underleverantör som agerar på den personuppgiftsansvariges instruktioner eller av en annan extern part. Den personuppgiftsansvarige som avser att stödja sin behandling på samtycket ansvarar dock för att samtycket uppfyller GDPR:s krav och ska kunna visa att ett giltigt samtycke har lämnats.[23]

Slutligen har den registrerade rätt att när som helst återkalla sitt samtycke. Det ska vara lika enkelt att återkalla samtycket som att lämna det. Om samtycket exempelvis lämnas genom ett val i en applikation eller på en webbplats bör det i praktiken kunna återkallas genom samma eller ett jämförbart gränssnitt. Ett återkallande påverkar inte lagligheten av den behandling som har utförts före återkallandet, men den behandling eller åtgärd som grundas på samtycket ska upphöra.[24]

---

[17] EDPB:s riktlinjer 05/2020, s. 16, p. 64.
[18] EDPB:s riktlinjer 05/2020, s. 16, p. 65.
[19] EDPB:s riktlinjer 05/2020, s. 18–19, p. 75–77.
[20] EU-domstolens dom den 11 november 2020, Orange România, C-61/19, EU:C:2020:901, p. 39.
[21] EDPB:s riktlinjer 05/2020, s. 20–21, p. 90.
[22] EDPB:s riktlinjer 05/2020, s. 21–22, p. 91–95.
[23] Artiklarna 5.2, 7.1 och 28.3 a GDPR. Jfr EDPB, riktlinjer 05/2020, punkt 65 och punkterna 104–108 om den personuppgiftsansvariges skyldighet att kunna visa att samtycke har lämnats.
[24] EDPB:s riktlinjer 05/2020, s. 24–25, p. 112–117.

4.5. GDPR och e-dataskyddsdirektivet – när gäller vilket regelverk?

FastrMobi utvecklar en digital tjänst vars grundläggande funktionalitet omfattar insamling av positioneringsuppgifter om användarens mobiltelefon genom mobiloperatörens mobilnät i syfte att aktivera tjänsten och för utskick av individanpassad information till användaren. För dessa funktioner behöver tjänsten behandla personuppgifter som kan innebära att både GDPR och e-dataskyddsdirektivet aktualiseras.

Platsbaserade tjänster
Platsbaserade tjänster kan användas inom en rad olika områden som till exempel detaljhandeln, hälso- och sjukvård samt nöjen och turism för att erbjuda skräddarsydda upplevelser och förbättrad service. För att sådana tjänster ska fungera behöver uppgifter om användarens geografiska position inhämtas.

Positioneringsuppgifter utgör personuppgifter
Uppgifter om en användares eller en mobiltelefons geografiska position utgör personuppgifter i GDPR:s mening när de kan knytas till en identifierad eller identifierbar fysisk person. Sådana uppgifter kan avslöja var en person befinner sig vid en given tidpunkt. Beroende på sammanhanget kan positioneringsuppgifter även avslöja sådana uppgifter som omfattas av artikel 9 GDPR, exempelvis uppgifter om hälsa, politiska åsikter eller religiös övertygelse (så kallade känsliga personuppgifter). Detta kan vara fallet när enskilda positionsuppgifter eller mer detaljerade rörelsemönster visar att en person har besökt exempelvis ett sjukhus, en religiös samlingsplats eller ett politiskt möte och därigenom avslöjar sådana förhållanden. Bedömningen behöver göras utifrån vad uppgifterna faktiskt avslöjar i sitt sammanhang. Om positioneringsuppgifterna utgör känsliga personuppgifter behöver även kraven i artikel 9 GDPR beaktas i den mån frågan inte regleras särskilt i e-dataskyddsdirektivet. När artikel 6 GDPR är tillämplig krävs både en rättslig grund enligt den artikeln och ett tillämpligt undantag enligt artikel 9.2. För sådan behandling gäller därmed strängare krav.[25]

Den beskrivna tjänstens användning av positioneringsuppgifter som kan knytas till en enskild användare innebär således behandling av personuppgifter. Positioneringsuppgifter kan samtidigt vara särskilt integritetskänsliga beroende på vad de visar och hur de kombineras med andra uppgifter. Nedan klargörs hur GDPR och e-dataskyddsdirektivet aktualiseras vid denna typ av behandling.

Tekniken som används påverkar vilket regelverk som är tillämpligt
Denna rapport avgränsas till fall där tjänsten automatiskt inhämtar positioneringsuppgifter om en användares mobiltelefon via en mobiloperatörs mobilnät samt fall där uppgifterna hämtas från mobiltelefonens terminalutrustning. En avgränsning görs mot andra situationer exempelvis i fall där besökaren via sin mobiltelefon besöker en webbplats, skannar en QR-kod på platsen eller ansluter till platsens Wi-Fi-nätverk.

Positioneringsuppgifter kan inhämtas på olika sätt och med hjälp av olika tekniker. Vilken teknik som används har betydelse för vilka regler, och därmed vilka materiella krav, som ska tillämpas. Bedömningen behöver också ta hänsyn till vilken typ av uppgifter som behandlas och för vilka ändamål.

Rapporten utgår från två scenarier. I det första sker positioneringen genom mobilnätet. I det andra hämtas positioneringsuppgiften från en mottagare i användarens

[25] Se EDPB:s riktlinjer 01/2020 om behandling av personuppgifter i samband med uppkopplade fordon och mobilitetsrelaterade tillämpningar, p. 63. Jfr EU-domstolens dom den 1 augusti 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, p. 119–128.

terminalutrustning, exempelvis genom GPS eller annat GNSS-system. Skillnaden mellan scenarierna är central för den efterföljande rättsliga bedömningen.

Scenario 1 - Inhämtning via mobilnätet
Ett sätt att identifiera var en användare befinner sig är genom positionering via mobilnätet. Positioneringsuppgifterna inhämtas av mobiloperatören, som kan fastställa telefonens position baserat på vilka basstationer enheten kommunicerar med.

Mobiloperatörens behandling av positioneringsuppgifterna för den digitala tjänsten sker för en annan tjänst än själva mobiltjänsten. För att avgöra vilken bestämmelse i e-dataskyddsdirektivet som är tillämplig behöver lokaliseringsuppgifter som samtidigt utgör trafikuppgifter skiljas från lokaliseringsuppgifter som inte är trafikuppgifter.

Trafikuppgifter är enligt artikel 2 b e-dataskyddsdirektivet uppgifter som behandlas för att överföra en kommunikation via ett elektroniskt kommunikationsnät eller för att fakturera den. Lokaliseringsuppgifter kan samtidigt vara trafikuppgifter. Skäl 35 anger att lokaliseringsuppgifter som behandlas i digitala mobilnät för att möjliggöra överföring av kommunikation utgör trafikuppgifter. I förarbetena nämns information om vilken nätcell en användare befinner sig i som exempel. Sådana uppgifter regleras av artikel 6 e-dataskyddsdirektivet. Andra lokaliseringsuppgifter, som inte är trafikuppgifter, kan omfattas av artikel 9.

Med mervärdestjänst avses enligt artikel 2 g en tjänst som kräver behandling av trafikuppgifter eller lokaliseringsuppgifter utöver vad som är nödvändigt för överföring eller fakturering av en kommunikation. Vid genomförandet i svensk rätt används uttrycket ”andra tjänster där uppgifterna behövs”, se 9 kap. 2 § LEK. Enligt förarbetena omfattar det samma tjänster som direktivets begrepp mervärdestjänst. Både artikel 6 och artikel 9 innehåller alltså regler om behandling för sådana tjänster.[26]

Om uppgifterna utgör trafikuppgifter regleras mobiloperatörens behandling för en mervärdestjänst av artikel 6.3, som har genomförts i 9 kap. 2 § andra stycket LEK. Behandlingen kräver samtycke och får endast ske i den utsträckning och under den tid som är nödvändig för tjänsten. Samtycket får när som helst återkallas. Bestämmelserna innehåller även krav på information och begränsningar av vilka som får behandla uppgifterna.

Om uppgifterna i stället utgör lokaliseringsuppgifter som inte är trafikuppgifter aktualiseras artikel 9, som har genomförts i 9 kap. 7–9 §§ LEK. Uppgifterna får då behandlas sedan de har avidentifierats eller användaren eller abonnenten har lämnat sitt samtycke. Behandlingen får endast ske i den utsträckning och under den tid som krävs för tjänsten.[27]

Kraven på samtycke enligt artiklarna 6.3 och 9 i e-dataskyddsdirektivet gäller även när uppgifterna är personuppgifter och GDPR därför också är tillämplig. Mobiloperatören kan alltså inte stödja behandlingen för en mervärdestjänst på någon annan rättslig grund enligt artikel 6.1 GDPR när direktivet kräver samtycke. I den frågan har direktivets särskilda regler företräde. För de frågor som inte regleras särskilt i direktivet gäller GDPR bestämmelser.[28]

[26] Prop. 2002/03:110, s. 258 och 260–261. Jfr artikel 2 b–c och g samt skäl 35 e-dataskyddsdirektivet.

[27] Artiklarna 6.3–6.5 och 9 e-dataskyddsdirektivet samt 9 kap. 2–3 och 7–9 §§ LEK.

[28] Se även EDPB:s yttrande 5/2019 om samspelet mellan e-dataskyddsdirektivet och GDPR, särskilt beträffande dataskyddsmyndigheternas behörighet, uppgifter och befogenheter, p. 38–41.

Scenario 2 - Inhämtning via GNSS-mottagare
Ett annat sätt att identifiera en användares position är genom mobiltelefonens inbyggda GNSS-mottagare och ibland i kombination med kringliggande trådlösa nät, vilket exempelvis kan ske via en applikation. Positioneringsuppgifterna kan inhämtas när applikationen används eller automatiskt i bakgrunden.

Den satellitbaserade positioneringen kräver inte nätverksuppkoppling. Uppkoppling via mobilnät eller Wi-Fi kan däremot behövas för att överföra positionen till eller använda positionen i den digitala tjänsten. Användaren behöver normalt även ha aktiverat funktionen för platstjänster i mobilen.

Trots att även detta scenario innebär en automatisk inhämtning av positioneringsuppgifter skiljer det sig från positionering via mobilnätet. Mobiloperatören är inte involverad i själva positioneringen och den digitala tjänsten hämtar positioneringsuppgiften från terminalutrustningen. Om applikationen får åtkomst till information som är lagrad i terminalutrustningen aktualiseras artikel 5.3 e-dataskyddsdirektivet, som i svensk rätt har genomförts i 9 kap. 28 § LEK. Bestämmelsen är inte begränsad till tillhandahållare av elektroniska kommunikationstjänster utan gäller alla som lagrar eller får tillgång till information i en användares terminalutrustning. Den gäller oavsett om informationen utgör personuppgifter.

Artikel 5.3 reglerar förutsättningarna för sådan lagring och åtkomst. Som huvudregel krävs att användaren har lämnat sitt samtycke. Undantag gäller för lagring eller åtkomst som behövs för överföring av ett elektroniskt meddelande eller är nödvändig för att tillhandahålla en tjänst på användarens eller abonnentens uttryckliga begäran. Huruvida något undantag är tillämpligt behöver bedömas utifrån den aktuella funktionen och ändamålet med åtkomsten.

I den mån informationen utgör personuppgifter har artikel 5.3 e-dataskyddsdirektivet företräde framför artikel 6.1 GDPR när det gäller själva lagringen eller åtkomsten. Tillhandahållaren av den digitala tjänsten måste således uppfylla kraven i artikel 5.3 och kan inte ersätta ett krav på samtycke enligt den artikeln med någon annan rättslig grund enligt GDPR. Den efterföljande behandlingen av personuppgifterna behöver bedömas separat.[29]

Samtycke och fortsatt behandling av positioneringsuppgifter
När e-dataskyddsdirektivet kräver samtycke för den aktuella behandlingen är det inte möjligt att ersätta detta krav med någon annan rättslig grund enligt GDPR. Kraven för ett giltigt samtycke hämtas från GDPR, vilket innebär att samtycket ska vara frivilligt, specifikt, informerat och otvetydigt.

Insamling, bearbetning och användning av positioneringsuppgifter utgör olika behandlingsmoment. Att uppgifterna används efter insamlingen innebär dock inte i sig att användningen sker för ett nytt ändamål. Om uppgifterna exempelvis samlas in och bearbetas för att välja ut och skicka platsanpassade erbjudanden kan momenten ingå i samma, närmare preciserade ändamål. Ett samtycke kan omfatta flera behandlingsmoment som tjänar samma ändamål, förutsatt att användaren får tillräcklig information om den behandling som samtycket omfattar.[30]

Även om momenten har samma ändamål behöver det bedömas vilka bestämmelser som gäller för respektive moment och aktör. Artiklarna 6 och 9 e-dataskyddsdirektivet kan reglera både insamling och fortsatt behandling av uppgifter för en mervärdestjänst. Artikel 5.3 reglerar däremot själva lagringen av eller åtkomsten till information i terminalutrustningen. Efterföljande behandling av personuppgifter behöver då som

[29] Se även EDPB:s yttrande 5/2019, p. 40–41.
[30] Skäl 32 GDPR. Se även EDPB:s riktlinjer 05/2020, s. 15, p. 57.

utgångspunkt ha en rättslig grund enligt GDPR.[31] Om uppgifterna används för elektronisk direktmarknadsföring behöver även de särskilda regler som beskrivs i avsnitt 4.6 nedan beaktas.

Att flera bestämmelser är tillämpliga innebär inte i sig att samtycke måste inhämtas vid olika tillfällen eller separat för varje behandlingsmoment. Ett gemensamt samtyckesförfarande kan användas, förutsatt att det uppfyller kraven enligt varje tillämplig bestämmelse. EDPB har uttryckligen angett att samtycke till åtkomst enligt artikel 5.3 e-dataskyddsdirektivet och samtycke till efterföljande behandling enligt GDPR för samma specifika ändamål kan inhämtas samtidigt.[32] Ett samtycke till positionering omfattar däremot inte automatiskt reklamutskick. För att samtyckesförfarandet ska omfatta båda leden behöver användaren tydligt kunna förstå och godta såväl positioneringen och användningen av uppgifterna som reklamutskicken. Om behandlingen tjänar flera särskilda ändamål ska användaren kunna ta ställning till dessa separat. Samtycket ska inhämtas innan den behandling som kräver samtycke påbörjas och kunna återkallas.

4.6. Individanpassad information till besökare

Vid individanpassad information behöver två behandlingsled skiljas åt. Det första avser behandlingar som sker före utskicket, exempelvis insamling och urval av kontaktuppgifter samt eventuell analys som används för att anpassa kommunikationen. Det andra avser själva det elektroniska utskicket. Vilka regler som gäller behöver bedömas separat för respektive behandlingsmoment.

För att kunna erbjuda individanpassad information behöver verksamheten behandla uppgifter om användaren. Det kan exempelvis röra sig om uppgifter om tidigare beteenden, information om användarens resväg eller syftet med ett besök för att kunna utforma innehållet på ett relevant sätt. Det gäller även behandlingen av användarens elektroniska kontaktuppgifter, vilka är nödvändiga för att informationen ska kunna levereras till rätt mottagare. Uppgifterna utgör personuppgifter.

Även vid den här typen av personuppgiftsbehandling kan både GDPR och e-dataskyddsdirektivet aktualiseras. Frågan är vilket regelverk som aktualiseras i samband med utskick av individanpassad information. E-dataskyddsdirektivet innehåller särskilda regler om elektronisk kommunikation för direkt marknadsföring i artikel 13. För utskick med elektronisk post, exempelvis e-post och sms, till fysiska personer gäller artikel 13.1 och 13.2, som i svensk rätt har genomförts i 19 § MFL. Huvudregeln är att ett giltigt samtycke från mottagaren måste ha inhämtats för att få göra utskicket om inte förutsättningarna för undantaget i artikel 13.2 är uppfyllda.[33]

Utöver reglerna om samtycke behöver även övriga tillämpliga krav i artikel 13 beaktas vid platsbaserad direktmarknadsföring. Enligt artikel 13.4 ska det exempelvis finnas en giltig adress dit mottagaren kan vända sig för att begära att utskicken upphör. Detta krav kommer till uttryck i 20 § MFL, enligt vilken meddelandet alltid ska innehålla en sådan adress vid marknadsföring med elektronisk post. Kravet gäller även när mottagaren har samtyckt till marknadsföringen.

Kommunikation för direktmarknadsföring är ett brett begrepp som inte bara omfattar uppenbar reklam, utan även exempelvis nyhetsbrev. Att informationen är

[31] Artiklarna 6.3–6.5 och 9 e-dataskyddsdirektivet. Se även EDPB:s riktlinjer 01/2020, p. 14–15, om artikel 5.3 e-dataskyddsdirektivet och efterföljande behandling enligt GDPR.

[32] EDPB:s riktlinjer 01/2020, p. 15 med fotnot 17. Uttalandet avser artikel 5.3 e-dataskyddsdirektivet och artikel 6 GDPR för samma specifika ändamål.

[33] En verksamhet som från sina kunder fått deras elektroniska kontaktuppgifter i samband med försäljning av en vara eller tjänst får använda uppgifterna för direkt marknadsföring utan samtycke i förväg, om kunden inte har motsatt sig detta och marknadsföringen avser verksamhetens egna, likartade varor eller tjänster. Kunden ska ges en tydlig, enkel och kostnadsfri möjlighet att motsätta sig användningen både vid insamlingen och vid varje följande meddelande. Se artikel 13.2 e-dataskyddsdirektivet och 19 § andra stycket MFL.

individanpassad eller skickas via RCS innebär dock inte i sig att den utgör direktmarknadsföring. Kommunikationens innehåll och syfte behöver bedömas.[34]

Som framgår av Inteligo-domen, som behandlas i avsnitt 4.3 ovan, reglerar artikel 13.2 de uttömmande förutsättningarna för den behandling som omfattas av bestämmelsen. Lagligheten av den behandlingen ska därför bedömas utifrån artikel 13.2 utan en parallell prövning enligt artikel 6.1 GDPR. När samtycke krävs enligt artikel 13.1 e-dataskyddsdirektivet kan det kravet inte ersättas med någon annan rättslig grund enligt GDPR.

Det är viktigt att skilja på själva utskicket och den förberedande behandlingen. Behandlingar som insamling av kontaktuppgifter och analys för individanpassning behöver bedömas separat enligt GDPR, i den mån de inte omfattas av särskilda regler i e-dataskyddsdirektivet. Gränsen mellan regelverken kan dock inte dras enbart utifrån om behandlingen sker före utskicket. Artikel 13.2 innehåller även villkor om hur kontaktuppgifterna har erhållits och om möjligheten att motsätta sig användningen redan vid insamlingen.

4.7. IMY:s kommentar

GDPR och e-dataskyddsdirektivet ska tillämpas parallellt när behandlingen omfattas av båda regelverken. Om e-dataskyddsdirektivet innehåller särskilda regler för ett visst behandlingsmoment gäller dessa framför motsvarande allmänna regler i GDPR. För frågor som inte regleras särskilt i e-dataskyddsdirektivet gäller GDPR som kompletterande regelverk.

Vilka regler som aktualiseras beror bland annat på hur uppgifterna inhämtas och behandlas. Vid positionering via mobilnätet behöver trafikuppgifter skiljas från lokaliseringsuppgifter som inte är trafikuppgifter. Mobiloperatörens behandling av uppgifter som kan knytas till en enskild användare för att tillhandahålla en mervärdestjänst kräver samtycke enligt artikel 6.3 eller artikel 9 e-dataskyddsdirektivet, beroende på uppgifternas karaktär. Åtkomst till positionsuppgifter i användarens terminalutrustning kan i stället omfattas av artikel 5.3. När e-dataskyddsdirektivet kräver samtycke kan detta krav inte ersättas med någon annan rättslig grund. Kraven för ett giltigt samtycke hämtas från GDPR.

Det är viktigt att skilja mellan olika behandlingsmoment och att samtidigt beakta vilka behandlingar de särskilda reglerna omfattar. Artiklarna 6 och 9 e-dataskyddsdirektivet kan även reglera fortsatt behandling för en mervärdestjänst. För efterföljande behandling av personuppgifter som har hämtats från terminalutrustning enligt artikel 5.3 behöver däremot som utgångspunkt en rättslig grund enligt GDPR fastställas. Att det är fråga om ett senare behandlingsmoment innebär inte automatiskt att ändamålet är nytt.

Samma princip gäller vid elektronisk direktmarknadsföring. De särskilda reglerna i e-dataskyddsdirektivet och MFL ska tillämpas på den kommunikation och de förutsättningar som de reglerar. Annan behandling, exempelvis analys och individanpassning, behöver bedömas separat enligt GDPR i den mån den inte omfattas av särskilda regler i e-dataskyddsdirektivet. Den rättsliga bedömningen behöver därför göras behandlingsmoment för behandlingsmoment och med hänsyn till den tekniska lösningen, uppgifternas karaktär och ändamålet med behandlingen.

[34] Enligt EU-domstolens praxis omfattar begreppet direktmarknadsföring kommunikationer som har ett kommersiellt syfte och riktas direkt och individuellt till en konsument. Även ett elektroniskt nyhetsbrev kan omfattas om kommunikationen har ett sådant kommersiellt syfte. Se EU-domstolens dom den 13 november 2025, Inteligo Media, C-654/23, EU:C:2025:871, punkterna 41–45.

5. Fördelning av ansvar enligt GDPR

I detta avsnitt analyseras ansvarsfördelningen enligt GDPR utifrån två scenarier för inhämtning av positioneringsuppgifter: via mobilnätet respektive via en GNSS-mottagare i användarens terminalutrustning. Scenarierna utgör utgångspunkt för bedömningen av ansvarsfördelningen enligt GDPR för de behandlingar som följer på inhämtningen, exempelvis tokenisering, hantering och överföring av uppgifter, matchning mot kundprofil samt hantering av samtycken och kundpreferenser. Avsnittet omfattar även ansvarsfördelningen för kommunikation med besökare och individanpassad information.

Avsnittet behandlar inte ansvarsfördelningen enligt LEK eller MFL. Dessa regelverk har egna bestämmelser och aktörsbegrepp. Att en aktör har en viss roll eller ett visst ansvar enligt dessa regelverk innebär därför inte automatiskt att aktören har motsvarande roll enligt GDPR.

Den materiella regleringen avseende personuppgiftsansvariga, personuppgiftsbiträden och gemensamt personuppgiftsansvariga har behandlats i tidigare rapporter.[35] Detta avsnitt ger enbart en kort sammanfattning av ansvarsfördelningen enligt GDPR för att direkt kunna gå in på de aktuella bedömningarna. För en mer utförlig genomgång hänvisas till tidigare rapporter.

5.1. Ansvarsroller enligt GDPR

Enligt artikel 4.7 GDPR är personuppgiftsansvarig den som, ensam eller tillsammans med andra, bestämmer ändamålen och medlen för behandlingen av personuppgifter. Med ändamål avses varför behandlingen sker, det vill säga syftet med behandlingen. Med medel avses hur behandlingen ska genomföras för att ändamålet ska uppnås.[36] En personuppgiftsansvarig är den som beslutar vissa nyckelelement i anslutning till behandlingen, framför allt behandlingens ändamål och väsentliga medel. Med väsentliga medel menas grundläggande beslut som har stor betydelse för hur personuppgifter behandlas, till exempel vilka uppgifter som samlas in, vilka personer som berörs och hur länge uppgifterna sparas.[37]

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning är enligt artikel 4.8 GDPR ett personuppgiftsbiträde. Det som kännetecknar ett personuppgiftsbiträde är alltså att aktören inte själv bestämmer ändamålen eller de väsentliga medlen för behandlingen. Personuppgiftsbiträdet utför i stället en behandling på uppdrag av den personuppgiftsansvarige.

Gemensamt personuppgiftsansvar föreligger enligt artikel 26.1 GDPR när två eller flera aktörer gemensamt fastställer ändamålen och medlen för en behandling. Det krävs alltså ett gemensamt inflytande över behandlingen, men inte nödvändigtvis att aktörerna påverkar alla delar av behandlingen i samma omfattning. EU-domstolen har i ett avgörande kommit fram till att en branschorganisation kan vara gemensamt personuppgiftsansvarig med sina medlemmar, i det fall organisationen inte enbart satt upp tekniska regler (till exempel hur systemet ska fungera) för sina medlemmar utan i detalj styrt hur de får lagra, dela och använda samtycken. För att gemensamt ansvar skulle uppstå krävdes att organisationen påverkade behandlingen för egna ändamål och därmed, tillsammans med medlemmarna, fastställde syftet och metoderna för behandlingen. Att organisationen inte själv hade direkt tillgång till personuppgifterna utgjorde inget hinder för att den skulle betraktas som gemensamt ansvarig. Det gemensamma ansvaret gällde bara för den behandling av personuppgifter som

[35] Se IMY, *Utlämnande av allmänna handlingar med hjälp av AI* (IMY-2024-5156), avsnitt 5.1, s. 23–26, samt IMY, *Ansvarsroller enligt GDPR vid finjustering av AI-applikationer* (IMY-2026-10502), avsnitt 2.3, s. 6–8.
[36] EDPB:s riktlinjer 07/2020 om begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, version 2.1, s. 15, p. 35.
[37] EDPB:s riktlinjer 07/2020, s. 12, p. 20 och s. 16, p. 40.

organisationen och medlemmarna bestämt tillsammans. Det gällde däremot inte automatiskt för senare behandlingar utförda av tredje part, såsom utskick av riktad reklam.[38]

Vilken teknisk funktion en aktör utför är därför inte i sig avgörande för rollen. Den tekniska arkitekturen är däremot viktig för att identifiera vilka behandlingar som sker och vilka beslut om ändamål och väsentliga medel som respektive aktör faktiskt har fattat.

5.2. Scenario 1 – Inhämtning via mobilnätet

I det första scenariot sker inhämtningen av positioneringsuppgifter via mobilnätet. Mobiloperatören utför den tekniska positioneringen av användarens mobiltelefon för att möjliggöra FastrMobis tjänst.

Inhämtningen av lokaliseringsuppgifter via mobilnätet aktualiserar särskilda regler enligt LEK. Denna reglering innebär inte i sig att ansvarsfördelningen enligt GDPR för de efterföljande behandlingarna är fastställd. Bedömningen enligt GDPR behöver därför avgränsas till de behandlingsmoment där förordningens regler om ansvarsfördelning är tillämpliga.

För de efterföljande behandlingarna behöver det bedömas vem som bestämmer ändamålen och de väsentliga medlen för respektive moment. Ett tydligt exempel rör tokeniseringen, FastrMobi skapar token och kan koppla en identifierad kund till en specifik token samt bestämmer hur länge kopplingen lagras. Detta talar för att FastrMobi bestämmer väsentliga medel för tokeniseringen och lagringen av kopplingen och därmed är personuppgiftsansvarig för dessa behandlingsmoment.

Om FastrMobi i stället behandlar personuppgifter enbart på uppdrag av butiken och enligt dess instruktioner, är bolaget personuppgiftsbiträde för dessa behandlingar. Om FastrMobi och butiken gemensamt bestämmer ändamål och väsentliga medel kan gemensamt personuppgiftsansvar aktualiseras. Mobiloperatörens roll enligt GDPR för eventuella efterföljande behandlingar behöver bedömas separat utifrån de faktiska omständigheterna. Att mobiloperatören utför den tekniska positioneringen innebär inte i sig att operatören är personuppgiftsbiträde enligt GDPR för samtliga behandlingsmoment i tjänsten.

5.3. Scenario 2 – Inhämtning via GNSS-mottagare

I det andra scenariot hämtas positioneringsuppgiften via en GNSS-mottagare i användarens terminalutrustning, exempelvis genom en funktion i en applikation. Mobiloperatören är då inte involverad i själva positioneringen inom ramen för den aktuella tjänsten.

Följaktligen kan den ansvarsfördelning som beskrivs för positionering via mobilnätet inte överföras direkt till detta scenario. Åtkomst till uppgifter i användarens terminalutrustning behöver bedömas mot de särskilda reglerna i LEK. GDPR-rollerna för den efterföljande behandlingen avgörs däremot av vem som bestämmer ändamål och väsentliga medel för respektive behandlingsmoment. Om FastrMobi även i detta scenario skapar token, kan koppla en identifierad kund till en specifik token och bestämmer hur länge kopplingen lagras, talar detta för att FastrMobi är personuppgiftsansvarig för dessa behandlingsmoment. Det innebär inte i sig att FastrMobi är personuppgiftsansvarig för varje moment i själva GNSS-inhämtningen.

Om butiken i stället bestämmer ändamål och väsentliga medel för den efterföljande behandlingen, exempelvis genom att bestämma vilka kunduppgifter som ska användas och hur de ska kopplas till kommunikationen, talar det för att butiken är

[38] EU-domstolens dom den 7 mars 2024, IAB Europe, C-604/22, EU:C:2024:214, punkt 78.

personuppgiftsansvarig för dessa behandlingsmoment. FastrMobi är då personuppgiftsbiträde i den utsträckning bolaget behandlar uppgifterna enbart på butikens uppdrag och enligt dess instruktioner.

Om FastrMobi tillsammans med butiken bestämmer ändamål och väsentliga medel för en viss behandling kan gemensamt personuppgiftsansvar aktualiseras. Om FastrMobi behandlar uppgifter för egna ändamål, exempelvis för att utveckla den egna tjänsten eller ta fram statistik för egna syften, behöver bolagets personuppgiftsansvar för dessa behandlingar bedömas separat.

Skillnaden mellan scenarierna är således främst hur positioneringsuppgiften hämtas och vilka aktörer som medverkar i det momentet. Denna skillnad kan påverka bedömningen av ansvarsfördelningen enligt GDPR, men avgör inte i sig vilka roller som aktörerna har för de efterföljande behandlingarna. Om samma aktörer fattar samma beslut om ändamål och väsentliga medel för de efterföljande behandlingarna kan ansvarsfördelningen enligt GDPR bli densamma i båda scenarierna.

5.4. Kommunikation med besökare och individanpassad information

Ansvarsfördelningen vid kommunikation med besökare behöver bedömas utifrån varje konkret behandlingsmoment och dess ändamål. Det bör särskilt skiljas mellan behandlingar som krävs för att möjliggöra kommunikationen, behandlingar som används för att koppla kommunikationen till en kundprofil och behandlingen som består i att utforma och skicka individanpassad information.

De behandlingar som kan ske inom ramen för att skicka individanpassad information kan exempelvis vara att kontrollera om kunden omfattas av tjänsten eller om kunden har lämnat relevant samtycke, matcha kommunikationen mot en kundprofil när det är aktuellt, välja vilket innehåll som ska skickas och slutligen genomföra själva utskicket.

Efter att kunden har detekterats kan FastrMobi kontrollera om kunden omfattas av tjänsten och, när det är relevant, om det finns ett registrerat samtycke som medger den aktuella kommunikationen. Uppgifter om samtycke och eventuell kundprofil kan hanteras inom FastrMobis tjänsteplattform. Att uppgifterna tekniskt hanteras i tjänsteplattformen är dock inte avgörande för ansvarsfördelningen. Rollen ska i stället bedömas utifrån vem som bestämmer ändamål och väsentliga medel för den aktuella behandlingen.

Om kunden *inte* väljer den funktion som innebär koppling till en kundprofil får butiken genom tjänsten endast tillgång till den information som behövs för den tokenbaserade kommunikationen. Kunden identifieras då inte genom den aktuella funktionen. Detta innebär dock inte att kunden nödvändigtvis är anonym för butiken, eftersom andra uppgifter eller informationskällor kan göra identifiering möjlig.

Om kunden i stället väljer en funktion som innebär att kommunikationen kopplas till en kundprofil kan tjänsteplattformen matcha den tokeniserade kommunikationen mot den registrerade kundprofilen. FastrMobi skapar token och kan koppla en identifierad kund till en specifik token samt bestämmer hur länge kopplingen lagras. Detta talar för att FastrMobi bestämmer väsentliga medel för behandlingen av kopplingen mellan kund och token och för hur länge den lagras. Butiken får då tillgång till information som gör det möjligt att koppla kommunikationen till en specifik kund. Den fortsatta behandlingen för att utforma och anpassa innehållet behöver bedömas separat utifrån de ändamål och väsentliga medel som butiken respektive FastrMobi bestämmer.

Ansvar för behandlingarna
Inom ramen för detta projekt är utgångspunkten att butiken har beslutat att kommunicera med besökare och har valt att använda FastrMobis tjänst för detta ändamål. Butiken

bestämmer dessutom innehållet i utskicken när kommunikationen ska individanpassas och vilka kunduppgifter som ska användas för att utforma kommunikationen. Dessa omständigheter talar för att butiken bestämmer ändamål och väsentliga medel för behandlingarna som avser att utforma och skicka den aktuella kommunikationen. Butiken är därmed personuppgiftsansvarig för dessa behandlingar.

Vilken roll FastrMobi har för behandlingar som föregår utskicket behöver bedömas separat för varje behandlingsmoment. Om butiken för över kunduppgifter till FastrMobi för att möjliggöra tjänsten och FastrMobi endast behandlar uppgifterna enligt butikens instruktioner, talar detta för en biträdesrelation. Om FastrMobi däremot tillsammans med butiken bestämmer ändamål och väsentliga medel för en behandling kan gemensamt personuppgiftsansvar aktualiseras. Det kan exempelvis bli fallet om FastrMobi påverkar vilka kunduppgifter som ska behandlas, hur de får delas eller hur de ska lagras.

FastrMobi kan även bli ensamt personuppgiftsansvarig om de vidarebehandlar kunduppgifterna för egna ändamål, exempelvis för att utveckla den egna tjänsten eller ta fram statistik för egna syften. I det fallet är FastrMobi ensam ansvarig för dessa efterföljande behandlingar. Biträdesansvar eller gemensamt ansvar kan däremot fortfarande föreligga för behandlingar i tidigare led.

5.5. IMY:s kommentar

I projektet har ansvarsfördelningen bedömts utifrån de konkreta behandlingar som aktualiseras i tjänsten. Bedömningen visar att den tekniska arkitekturen och det ändamål för vilket en uppgift behandlas har betydelse för vilken roll respektive aktör får.

Scenario 1, vid inhämtning av positioneringsuppgifter via mobilnätet behöver de särskilda reglerna i LEK om lokaliseringsuppgifter beaktas. GDPR-rollerna för efterföljande behandlingar ska bedömas separat. FastrMobi skapar token, kan koppla en identifierad kund till en specifik token och bestämmer hur länge kopplingen lagras. Detta talar starkt för att FastrMobi är personuppgiftsansvarig för dessa behandlingsmoment, i den mån GDPR är tillämplig.

Scenario 2, vid inhämtning via GNSS är mobiloperatören inte involverad i själva positioneringen, men även där avgörs GDPR-rollerna för efterföljande behandlingar av vem som bestämmer ändamål och väsentliga medel. Skillnaden mellan scenarierna ändrar alltså inte automatiskt ansvarsfördelningen för tokenisering, kundkoppling och lagring.

För den kommande kommunikationen med besökare behöver ansvarsfördelningen bedömas utifrån det specifika behandlingsmomentet. Butiken bestämmer innehållet i kommunikationen och, när kommunikationen ska individanpassas, vilka kunduppgifter som ska användas för detta ändamål. Detta talar starkt för att butiken är personuppgiftsansvarig för dessa behandlingar. Vilken roll FastrMobi har för behandlingar som föregår kommunikationen är beroende av om FastrMobi behandlar uppgifter endast på uppdrag av butiken, har påverkat behandlingen eller behandlar uppgifterna för egna syften.

Sammanfattningsvis kan samma aktör omfattas av olika skyldigheter och ha olika roller i skilda regelverk och för olika behandlingsmoment. Den rättsliga bedömningen behöver därför utgå från det konkreta momentet, dess ändamål, den tekniska utformningen och de regler som är tillämpliga.

6. Övriga reflektioner

Inför en eventuell driftsättning behöver den faktiska tekniska lösningen verifieras mot den tekniska lösning som har analyserats i denna rapport. Det gäller bland annat hur kunder som omfattas av tjänsten avgränsas i mobilnätet, när mobilnumret ersätts med en token, vilka uppgifter som lämnar mobiloperatörens miljö, hur matchning mot kundprofil sker och hur kundens val och återkallanden hanteras.

Vidare behöver ansvarsfördelningen omsättas i den faktiska avtals- och informationsstrukturen mellan aktörerna. Den som är personuppgiftsansvarig för respektive behandling behöver kunna visa att behandlingen har en tillämplig rättslig grund och att kraven på information, säkerhet, lagring och hantering av registrerades rättigheter är uppfyllda.

Den tekniska och organisatoriska utformningen bör också verifieras så att tokenisering och informationsseparation används konsekvent och så att direkt identifierande uppgifter inte exponeras för aktörer som inte behöver dem för att utföra sin del av tjänsten.

7. Fördjupning

Detta avsnitt samlar vägledningar för den som vill fördjupa sig utöver vad som behandlas i rapporten. Hänvisningarna pekar på material som utvecklar relevanta begrepp, metodik och praktisk tillämpning.

För vägledning om rollerna personuppgiftsansvarig, gemensam personuppgiftsansvarig och personuppgiftsbiträde samt gränsdragningen mellan dessa hänvisas till EDPB:s riktlinjer 07/2020.

Vägledning kring begreppen anonymisering och pseudonymisering hänvisas till EDPB:s riktlinjer 02/2026 samt 01/2025. Dessa riktlinjer är vid datumet för publiceringen av denna rapport inte slutligt antagna.

Vägledning kring det tekniska tillämpningsområdet för artikel 5.3 e-dataskyddsdirektivet hänvisas till EDPB:s riktlinjer 2/2023.

Ytterligare vägledning kring samspelet mellan GDPR och e-dataskyddsdirektivet hänvisas till EDPB:s yttrande 5/2019.

Nedan listas slutrapporter från projekt i IMY:s innovationssandlåda om dataskydd. Hänvisningarna avser vidare läsning och fördjupning utöver vad som behandlas i denna rapport. För en uppdaterad sammanställning av publicerade sandlåderapporter, se IMY:s innovationsportal.

Publicerade slutrapporter

- Utlämnande av allmänna handlingar med hjälp av AI, 7 november 2024 (IMY-2024-5156).
- Delning av kunduppgifter mellan banker i syfte att motverka ekonomisk brottslighet, 19 maj 2025 (IMY-2024-14275).
- Vidarebehandling av personuppgifter i vårdnadsärenden för att träna en AI-modell, 9 december 2025 (IMY-2025-23536).
- Betrodda exekveringsmiljöer för uppkopplade fordon, 30 mars 2026 (IMY-2026-5444).
- Transkribering inom socialtjänsten, 13 april 2026 (IMY-2026-6527).

IMY. Integritetsskydds myndigheten

Detta är Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten (IMY) arbetar för att skydda dina personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer.

Vi är Sveriges dataskyddsmyndighet. Det är vi som kontrollerar att företag och myndigheter följer dataskyddsförordningen GDPR. Vi vägleder dem som behandlar personuppgifter, för att göra det lättare att göra rätt och för att främja innovation där rättigheter och effektivitet står i balans. Tillsammans med övriga dataskyddsmyndigheter i EU arbetar vi för att medborgarnas personuppgifter ska ha samma skydd i hela unionen. Genom vårt arbete bidrar vi till ett tryggare digitalt Sverige, där människor har tillit till att deras personuppgifter hanteras som de ska och samhällets motståndskraft är stark.

Kontakta Integritetsskyddsmyndigheten

E-post: imy@imy.se
Webb: www.imy.se
Tel: 08-657 61 00
Postadress: Integritetsskyddsmyndigheten,
Box 8114, 104 20 Stockholm