



Rapportnummer

PTS

PTS-ER-2010:01

Datainspektionen

2010:1

Datum

2010-01-19

# Användning av trafikuppgifter i mobila innehållstjänster

Rapport efter avslutad tillsyn



## **Användning av trafikuppgifter i mobila innehållstjänster**

Rapport efter avslutad tillsyn

### **PTS rapportnummer**

PTS-ER-2010:01

### **Datainspektionens rapportnummer**

2010:1

### **PTS diarienummer**

09-5636

### **Datainspektionens diarienummer**

1128-2009

### **ISSN**

1650-9862

### **Författare**

Rapporten har sammanställts gemensamt av PTS och Datainspektionen. För PTS räkning har Per Bergstrand, Erika Hersaeus och Staffan Lindmark deltagit. För Datainspektionens räkning har Jonas Agnvall, Lena Carlsson, Mikael Ejner och Adolf Slama deltagit.

### **Post- och telestyrelsen**

Box 5398

102 49 Stockholm

08-678 55 00

[pts@pts.se](mailto:pts@pts.se)

[www.pts.se](http://www.pts.se)

### **Datainspektionen**

Box 8114

104 20 Stockholm

08-657 61 00

[datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se)

[www.datainspektionen.se](http://www.datainspektionen.se)

## Förord

Mobiltelefonen är inte längre bara en enhet för att utföra röstsamtal, utan är en plattform för kommunikation och tjänster av alla slag. Den tekniska utvecklingen skapar goda möjligheter och incitament att i snabb takt utveckla nya tjänster för mobiltelefoner. Den ännu unga marknaden för mobila innehållstjänster präglas därför av innovation. Marknadens möjligheter har ökat också genom att samarbeten mellan olika aktörer i branschen har etablerats, inte minst vad gäller utbyte av information, såsom uppgifter om mobilanvändarna.

Det är dock viktigt att denna i stort positiva utveckling sker med hänsyn tagen till användarnas rättigheter. I den här rapporten analyseras tillämpningen av de regler till skydd för den personliga integriteten som måste beaktas när uppgifter om mobilanvändare överförs mellan aktörerna på marknaden för mobila innehållstjänster.

Dessa regler återfinns i två olika lagstiftningar, med kommunikationsmyndigheten PTS (PTS) respektive Datainspektionen som ansvarig myndighet. Rapporten har därför tagits fram i samarbete mellan myndigheterna. Ambitionen med rapporten är att överbrygga de frågeställningar som naturligt uppstår när överlappande lagstiftningar med skilda tillsynsmyndigheter ska hanteras av marknadens aktörer.

Katarina Kämpe  
Stf generaldirektör, PTS

Göran Gräslund  
Generaldirektör, Datainspektionen

# Innehåll

<b>Förord</b>	<b>3</b>
<b>Sammanfattning</b>	<b>6</b>
<b>Abstract</b>	<b>8</b>
<b>1 Inledning</b>	<b>10</b>
1.1 Bakgrund till granskningen av marknaden för mobila innehållstjänster	10
1.2 Två myndigheter - en rapport	12
1.2.1 Kort om PTS och Datainspektionen	12
1.2.2 Syftet med de genomförda tillsynsinsatserna	12
1.2.3 Rapportens disposition, avgränsningar och metod	13
<b>2 Lagstiftningen om behandling av uppgifter</b>	<b>15</b>
2.1 Definitioner och begrepp	16
2.2 Lagen om elektronisk kommunikation	16
2.3 Personuppgiftslagen	19
<b>3 Användning av uppgifter i mobila innehållstjänster</b>	<b>23</b>
3.1 Allmänt om mobila innehållstjänster och dess leverantörer	23
3.2 Operatörers och aggregatörers roll på marknaden	24
3.3 Användningen av lokaliseringssuppgifter	27
3.4 Aktörernas reglering av behandlingen	28
<b>4 Bedömning av behandlingen av uppgifter för mobila innehållstjänster</b>	<b>31</b>
4.1 Vilken lag ska tillämpas på behandlingen?	32
4.2 Vem ansvarar för att bestämmelserna i PuL följs?	33
4.3 När krävs samtycke för att behandlingen ska vara tillåten?	34
4.3.1 Operatörer	34
4.3.2 Innehållsleverantören	38
4.3.3 Aggregatören	39
4.4 Uppfylls övriga krav på behandlingen?	39
<b>5 Säkerheten vid överföring av uppgifter</b>	<b>43</b>
5.1 Regleringen om skydd av uppgifter i mobila innehållstjänster	44
5.2 Grundläggande principer för skydd av information vid överföring och lagring	45
5.3 Kommunikationen mellan aktörerna och de tekniker som används	47
5.4 Tekniska åtgärder för att skydda uppgifter vid överföring och vid lagring	49
<b>6 Slutsatser och rekommendationer</b>	<b>51</b>
6.1 Rekommendationer för ökad hänsyn till integritet	52
6.1.1 Telefonnummer bör undvikas för identifiering	52
6.1.2 Integritet bör beaktas redan när tjänster tas fram	53
6.1.3 Aktörerna bör se över rutiner för samtycke och information	54
6.2 Rekommendationer för ökad säkerhet vid överföring av uppgifter	55
6.2.1 Informationsklassning och riskanalyser bör genomföras	55
6.2.2 Åtkomsträttigheter bör begränsas och autentisering användas	55
6.2.3 Kryptering bör användas när trafikuppgifter överförs	55
6.2.4 Autentisering och transaktioner bör loggas	55
<b>7 Myndigheternas fortsatta arbete</b>	<b>57</b>
7.1 PTS fortsatta arbete	57
7.2 Datainspektionens fortsatta arbete	58
<b>Litteratur</b>	<b>59</b>

## Bilagor

Bilaga 1 – Definitioner och förklaring av grundläggande begrepp	60
Bilaga 2 – Utdrag ur relevant lagstiftning	62
Bilaga 3 – Gränsdragningen mellan LEK och PuL	70
Bilaga 4 – Schematisk bild över gränsdragningen mellan LEK och PuL	78
Bilaga 5 - Tekniska begrepp	79

## Sammanfattning

PTS och Datainspektionen har gemensamt utrett hanteringen av trafikuppgifter i mobila innehållstjänster, som ett led i respektive myndighets ambition att genom samarbete nå ökad tydlighet. Området är komplicerat: dels för att det är det tekniskt komplext och dels eftersom det finns två överlappande lagstiftningar på området: lagen (2003:389) om elektronisk kommunikation (LEK) och personuppgiftslagen (1998:204) (PuL), som därtill har olika myndigheter på vilka tillsynsansvaret ligger.

Rapporten har föregåtts av en generell granskning där ett antal operatörer, aggregatörer och innehållsleverantörer genom skriftliga frågor besvarat hur de använder trafikuppgifter vid tillhandahållandet av mobila innehållstjänster. Denna granskning ligger till grund för såväl utredningen om hur marknaden tekniskt fungerar samt de slutsatser och rekommendationer som ges. I förekommande fall ges även reflektioner över hur aktörerna som grupp svarat. Den utförda granskningen har dock inte i första hand varit avsedd att ligga till grund för en bedömning i de enskilda fallen. Snarare har syftet varit att samla fakta som myndigheterna kunnat utgå från i sina resonemang kring lagkrav och behov av säkerhetsåtgärder.

I sammanhanget ska nämnas att marknaden som sådan är förhållandevis ung. Därför bör den behandlas på ett sätt och med medel som gör det möjligt för den att växa, samtidigt som de bestämmelser och rekommendationer tillvaratas, som syftar till att skydda användarnas integritet och därmed också på sikt tilliten till tjänsterna.

Myndigheterna har funnit att hanteringen av trafikuppgifter överlag fungerar tillfredsställande. Aktörernas uppfattning om vilka regelverk som omfattar deras verksamhet är dock skiftande, vilket är olyckligt eftersom detta också innebär att det kan finnas en osäkerhet om var ansvaret för hanteringen ligger. Granskningen av innehållsleverantörer har visat att den information som de lämnar till de registrerade kan förbättras i flera avseenden, bl.a. vad gäller rätten till registerutdrag och möjligheten att begära rättelse, liksom beskrivningen av ändamålen med behandlingen.

Myndigheterna har därför sett ett behov av att tydligt redogöra för den reglering som är tillämplig samt hur denna reglering bör tillämpas avseende den faktiska hantering av uppgifter som sker. Rapporten innehåller rekommendationer kring lämpligheten av att använda telefonnummer som identifiering, information i samband med samtycke och rekommendationer för ökad säkerhet vid överföring av uppgifter. Rekommendationerna ges som en ambition att uppnå målet, att den växande marknaden för mobila innehållstjänster tillvaratar såväl användarnas behov av avancerat innehåll som deras behov av integritetsskydd och säkerhet. Myndigheternas förhoppning är

att denna rapport utgör ett steg mot detta mål och myndigheterna kommer att fortsätta att följa utvecklingen inom området för mobila innehållstjänster.

## Abstract

PTS and the Swedish Data Inspection Board have jointly investigated the processing of traffic data in mobile content services as a step in these authorities' ambition to achieve a greater level of clarity through collaboration. This area is complicated: first because it is technically complex, and second because there are two competing statutes in this field, namely the Electronic Communications Act (2003:389 – LEK) and the Personal Data Act (1998:204 – PuL), in which connection different authorities are responsible for supervision and compliance.

This report was preceded by a general study, where a number of operators, aggregators and content suppliers responded to written questions about how they use traffic data when providing mobile content services. This study forms the basis of the survey of how the market functions from a technical perspective as well as the conclusions and recommendations made. When applicable, reflections are also presented concerning how the stakeholders have responded as a group. However, the study conducted was not primarily intended to provide a basis for assessing individual cases; rather, the aim was to compile facts on which the authorities could base their reasoning about the need for legislation and security measures.

It should also be mentioned in this context that the market as such is rather immature. It should consequently be dealt with in such a way and using means that enable growth while also observing the rules and recommendations aimed at protecting the privacy of users and thus also confidence in these services in the long run.

The authorities found that, on the whole, the stakeholders manage traffic data processing in a satisfactory manner. However, stakeholders had differing perceptions of which systems of rules covered their operation, which is unfortunate as this also means that there may be some uncertainty about where the responsibility for processing lies. The study of content suppliers showed that the information provided by them to data subjects can be improved in several respects; for example, regarding the right to receive extracts from records and the possibility of requesting rectification, and similarly having the purpose of the processing explained.

The authorities have therefore identified a need to clearly explain the applicable regulatory provisions and also how such regulation should be applied in terms of the processing of data that takes place in practice. This report includes recommendations concerning the appropriateness of using telephone numbers as identification, information in conjunction with consent and recommendations for enhanced security when transferring data. The aim of these recommendations is to achieve the following objective: that the growing

market for mobile content services fulfils both the users' need for advanced content and their need to protect their privacy and security. The authorities hope that this report represents a step towards achieving this objective and will continue to observe how the market develops.

# 1 Inledning

## Sammanfattning

Mobiltelefoner används idag för en lång rad tjänster som nyttjar olika former av trafikuppgifter och lokaliseringssuppgifter som en del av tjänsten eller för att kunna betala för tjänsten. Det är viktigt att den ökade behandlingen av personuppgifter som behövs för att möjliggöra många mobila innehållstjänster inte sker på bekostnad av den personliga integriteten.

Hanteringen av uppgifterna regleras såväl i LEK som PuL, regelverk som har olika tillsynsmyndigheter. Detta komplicerar frågan om gränsdragningen mellan de båda lagarna och därmed också frågan om ansvaret för hanteringen.

Under våren och hösten 2009 har PTS och Datainspektionen gemensamt genomfört en undersökning i syfte att utreda bl.a. vilka uppgifter som överförs mellan aktörerna och även göra generella bedömningar av vilken lagstiftning som gäller för den aktuella behandlingen av uppgifter. Samarbetet mellan myndigheterna har gett möjligheter att göra bedömningar avseende behandlingen av uppgifter i hela kedjan från operatör, via aggregatör till innehållsleverantör.

## 1.1 Bakgrund till granskningen av marknaden för mobila innehållstjänster

Mobiltelefoner används inte längre till att enbart ringa samtal och skicka textmeddelanden. Många av de mobiltelefoner som säljs idag innehåller även t.ex. kalender- och spelprogramvara, musikspelare, kamera, GPS-mottagare och webbläsare. Mer avancerade telefoner har operativsystem som ger användaren stora möjligheter att anpassa telefonens innehåll genom att installera egen programvara och på olika sätt anpassa telefonens användargränssnitt. Men även till de enklare telefonerna kan vanligen innehåll, i form av ringsignaler och bilder liksom enklare spel och nyttoprogram, hämtas.

De ökade möjligheterna att på olika vis anpassa mobiltelefonen med innehåll från andra parter än telefontillverkaren, har under senare år bidragit till framväxten av ett stort antal tjänster som tillhandahåller innehåll av varierande slag. Många av dessa innehållstjänster erbjuder innehåll till mobiltelefonen som kan hämtas via Internet alternativt genom sms- eller mms-meddelanden. Till innehållstjänsterna räknas även alla de tjänster som inte främst erbjuder

nedladdning av information utan där tjänsten tillhandahålls över Internet och nås av användaren via t.ex. mobiltelefonens wap- eller webbläsare.

Begreppet mobila innehållstjänster är således mycket omfattande och innefattar bl.a. tjänster för försäljning av ringsignaler, spel och musik, nyhets- och vädertjänster, abonnentupplysning, karttjänster, sociala nätverkstjänster och tjänster för strömmande video.

Kännetecknande för många av de mobila innehållstjänsterna är att de är uppbyggda så att de ska gå snabbt och enkelt att använda via mobiltelefonens begränsade användargränssnitt och över en långsam uppkoppling. Tjänsterna används typiskt sett i miljöer och sammanhang som ställer krav på att det eftersökta innehållet ska kunna nås av användaren i ett fåtal enkla moment. Komplexa procedurer, för t.ex. inloggning eller betalning, kan befaras minska nyttan och därmed efterfrågan på tjänsterna.

De innehållsleverantörer som vill ta betalt för det erbjudna innehållet har därför sett ett behov av att utveckla effektiva betalningslösningar. Sådana lösningar har förverkligats genom ett samarbete med mobiloperatörerna. Operatören har en existerande kundrelation med användaren och kan, tack vare att all trafik till och från mobiltelefonen passerar genom operatörens nät, identifiera och debitera användaren för innehåll som denne beställer via en innehållstjänst. Förfarandet beskrivs utförligare nedan, i 3.2.

Operatörernas roll i tillhandahållandet av innehållstjänster har ytterligare utvecklats, i och med uppkomsten av tjänster som bygger på information om var användaren befinner sig, s.k. lokaliseringssuppgifter. Sådana uppgifter används i mobilnäten för att möjliggöra trafikdirigering men kan nu även göras tillgängliga för innehållsleverantörer som har behov av uppgifterna i sina tjänster. Det kan t.ex. röra sig om tjänster som tillhandahåller kartor eller abonnentupplysning där sökresultat anpassas till det geografiska närområdet.

För att möjliggöra betalning eller lokalisering i en mobil innehållstjänst utbyts alltså information om användarens identitet och position mellan operatörer och innehållsleverantörer. Eftersom det finns ett flertal operatörer kan det vara problematiskt för innehållsleverantörer att anpassa teknik och avtal för samtliga operatörer. En marknad har därför uppstått för mellanhänder, s.k. aggregatörer, som tillhandahåller gränssnitt mellan operatörer och innehållsleverantörer.

Det är viktigt att den ökade behandlingen av personuppgifter som behövs för att möjliggöra många mobila innehållstjänster inte sker på bekostnad av den

personliga integriteten. Under 2008 uppmärksammades i media att den som använder Internet i sin mobiltelefon i många fall är omedveten om att bl.a. dennes telefonnummer lämnas ut till vissa webbplatser som besöks. Det rapporterades också om misstag i den tekniska utformningen av en tjänst som bygger på lokaliseringuppgifter, vilket lett till att det varit möjligt för användare att via tjänsten ta reda på någon annans position.

## **1.2 Två myndigheter - en rapport**

### **1.2.1 Kort om PTS och Datainspektionen**

#### PTS

PTS är den myndighet som bevakar områdena elektronisk kommunikation och post i Sverige. PTS utövar tillsyn enligt LEK. LEK är en sektorspecifik lagstiftning som innehåller specialreglering för olika former av behandlingar som sker inom ramen för tillhandahållandet av en elektronisk kommunikationstjänst.

#### Datainspektionen

Datainspektionen är en central förvaltningsmyndighet som genom sin tillsynsverksamhet ska bidra till att behandlingen av personuppgifter inte medför otillbörligt intrång i enskildas personliga integritet. Målet ska nås utan att användningen av teknik onödigt hindras eller försvåras.

Datainspektionen är tillsynsmyndighet över sådan personuppgiftsbehandling som regleras av PuL. Syftet med PuL är att skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter.

### **1.2.2 Syftet med de genomförda tillsynsinsatserna**

Under våren och hösten 2009 har PTS och Datainspektionen gemensamt genomfört en undersökning av mobiloperatörer respektive innehållsleverantörer och aggregatörer, i syfte att utreda bl.a. vilka uppgifter som överförs mellan aktörerna och behandlas för att stödja mobila innehållstjänster, hur och under vilka förutsättningar denna behandling sker samt vilka kontrollmekanismer som tillämpas för att avgränsa spridningen och användningen av uppgifterna till vad som är nödvändigt för ändamålet.

Syftet har vidare varit att göra bedömningar av vilken lagstiftning som gäller för den aktuella behandlingen av uppgifter och hur lagstiftningen ska tillämpas. Samarbetet mellan myndigheterna har gett möjligheter att göra bedömningar

avseende behandlingen av uppgifter i hela kedjan från operatör, via aggregatör till innehållsleverantör.

Rapporten redogör för de uppgifter som framkommit i tillsynsarbetet och de slutsatser som myndigheterna har dragit gällande behandlingen. Avsikten är att dessa slutsatser ska tjäna som vägledning för aktörerna på marknaden för dess vidare utveckling.

### **1.2.3 Rapportens disposition, avgränsningar och metod**

#### Rapportens disposition

Rapporten redogör inledningsvis närmare för de aktörer på marknaden för mobila innehållstjänster som nu varit föremål för tillsyn och relationerna dem emellan samt branschpraxis. Vidare redogörs kortfattat för de förlopp, i vilka uppgifter om användare eller abonnenter överförs mellan eller används av aktörerna.

Härefter redovisas de rättsliga aspekterna på behandlingen av uppgifterna varvid myndigheternas bedömning av gränsdragningsfrågor vad gäller tillämpligheten av LEK och PuL redovisas. I detta kapitel återfinns också en genomgång av praktiska frågor kring samtycke uppdelat på operatörer, innehållsleverantörer respektive aggregatörer. Kapitlet avslutas med en redogörelse för myndigheternas bedömningar avseende den aktuella behandlingen av uppgifter för mobila innehållstjänster.

Ett särskilt kapitel ägnas åt de tekniska och organisatoriska säkerhetsåtgärder som marknadsaktörer tillämpar för att upprätthålla de behandlade uppgifternas riktighet, tillgänglighet och konfidentialitet. Myndigheterna redogör i kapitlet även för generella säkerhetsprinciper för behandling av personuppgifter och hur dessa principer kan tillämpas av aktörerna på marknaden för mobila innehållstjänster.

Härefter följer ett kapitel med myndigheternas samlade slutsatser och rekommendationer avseende olika aspekter på behandling av uppgifter vid mobila innehållstjänster.

Rapporten avslutas med en beskrivning av hur myndigheterna avser att fortsätta arbetet inom området.

#### Avgränsningar

Rapporten, liksom den tillsyn som genomförts, berör endast integritets- och säkerhetsaspekter på den överföring och annan behandling som operatörer,

aggregatörer och innehållsleverantörer, som är etablerade i Sverige, utför i samband med tillhandahållandet av mobila innehållstjänster.

Behandling som sker utöver den mobila innehållstjänsten (t.ex. behandling i kundregister och liknande) faller utanför rapporten.

Rapportens bedömningar avser endast uppgiftsbehandling enligt LEK och PuL. Det bör dock påpekas att det finns andra bestämmelser som aktörerna måste ta hänsyn till, t.ex. konsumenträttsliga regler om tydlighet och villkor i avtal. Sådana frågor har dock inte behandlats inom ramen för den aktuella tillsynen och beaktas därför inte heller i denna rapport.

#### Metod

PTS har, inom ramen för sin tillsyn, genom en enkät till ett urval av mobiloperatörer, inhämtat uppgifter om operatörernas behandling av abonnent- och lokaliseringsuppgifter för användning i mobila innehållstjänster. Datainspektionen har på samma vis inhämtat uppgifter från ett fåtal aggregatörer och innehållsleverantörer. Faktauppgifter i rapporten bygger huvudsakligen på de enkätsvar som marknadsaktörerna har lämnat till myndigheterna.

För de juridiska bedömningarna avseende tillämpningen av LEK respektive PuL svarar respektive myndighet. De rekommendationer som lämnas i rapporten bygger på tillämplig författning samt myndigheternas tidigare tillsyns- och utredningsarbete inom området.

## 2 Lagstiftningen om behandling av uppgifter

### Sammanfattning

---

Det finns i huvudsak två lagar att ta hänsyn till när det gäller behandling av trafikuppgifter såsom t.ex. lokaliseringssuppgifter vid nyttjandet av tjänster över mobila nät. Dessa är personuppgiftslagen (PuL) och lagen om elektronisk kommunikation (LEK). LEK är en speciallagstiftning som gäller före den generella lagstiftningen PuL, vilket innebär att om något är särskilt reglerat i LEK så gäller inte PuL i dessa situationer.

Behandling av trafikuppgifter och utbyte av sådana uppgifter regleras främst genom två lagar: lagen (2003:389) om elektronisk kommunikation (LEK) och personuppgiftslagen (1998:204) (PuL). Båda lagarna bygger på EG-direktiv.<sup>1</sup> I det här kapitlet redogörs för hur lagbestämmelserna tillämpas generellt. I kapitel 4.1 redogörs för PTS och Datainspektionens bedömningar av hur bestämmelserna ska tillämpas på överföringen av trafikuppgifter för mobila innehållstjänster.

LEK är en sektorspecifik lagstiftning som innehåller specialreglering för olika former av behandlingar som sker inom ramen för tillhandahållandet av en elektronisk kommunikationstjänst. I 6 kapitlet LEK regleras integritetsfrågor, såsom operatörernas hantering av trafikuppgifter. Syftet med integritetskapitlet i LEK är att skydda användare av elektroniska kommunikationstjänster då dessa tjänster ansetts så pass viktiga och förmedla så pass mycket information av integritetskänslig natur.

PuL reglerar behandling och hantering av personuppgifter i allmänhet. Syftet med PuL är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. PuL utgör en så kallad subsidiär lagstiftning. Detta innebär att om det finns en annan mer specifik lag som reglerar hanteringen av personuppgifterna så har denna lag företräde. Mycket förenklat kan därför sägas att i den utsträckning LEK reglerar hanteringen eller

---

<sup>1</sup> De integritetsrelaterade bestämmelserna i 6 kapitlet lagen om elektronisk kommunikation bygger huvudsakligen på 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). Personuppgiftslagen bygger på Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

behandlingen av trafikuppgifter i mobila innehållstjänster så gäller denna lag och där så inte är fallet gäller istället PuL.

I praktiken kan dock gränsdragningar i flera fall vara svåra att göra; särskilt när flera parter är inblandade i uppgiftsutbytet, varav vissa tillhandahåller elektroniska kommunikationstjänster i LEKs bemärkelse (såsom operatörerna) medan andra inte gör det (såsom innehållsleverantörerna).

I de följande avsnitten ges en översiktlig genomgång av de regler som avser behandling av uppgifter i LEK och PuL.

## **2.1 Definitioner och begrepp**

I rapporten beskrivs och bedöms den hanteringen och överföring som sker av vissa uppgifter, såsom t.ex. telefonnummer och positionsuppgifter, från ursprunget i mobilnäten till mobila innehållstjänster. Som framgår nedan i bilaga 1 – ”Definitioner och förklaring av grundläggande begrepp” – omfattas denna behandling av uppgifterna av två olika lagar, vars begreppsapparat skiljer sig åt.

Detta innebär att samma uppgift, beroende på sammanhang, kan komma att omfattas av fler än ett begrepp. Som exempel kan ett telefonnummer under vissa förutsättningar anses utgöra såväl en ”trafikuppgift” som en ”personuppgift”.

En förteckning över definitioner och förklaring av begrepp som används i rapporten återfinns i bilaga 1.

## **2.2 Lagen om elektronisk kommunikation**

I detta avsnitt introduceras de bestämmelser i 6 kapitlet LEK som reglerar behandling av abonnent-, trafik- och lokaliseringssuppgifter och de generella förutsättningarna för utlämnande av sådana uppgifter.

Bestämmelserna avser särskilda kategorier av uppgifter

Reglerna omfattar endast behandling av vissa särskilt angivna kategorier av uppgifter. Det rör sig om

- abonnentuppgifter,
- trafikuppgifter,
- lokaliseringssuppgifter som inte utgör trafikuppgifter, samt
- innehåll i de meddelanden som överförs genom elektroniska kommunikationstjänster.

Kategoriseringen av en viss uppgift är beroende av det sammanhang där uppgiften förekommer. Med abonnentuppgifter avses uppgifter som kan användas för att identifiera och hitta eller på något sätt kontakta en abonnent, och som är relativt statiskt kopplade till abonnenten. Trafikuppgifter avser istället sådana uppgifter som inte främst är kopplade till abonnenten utan till kommunikationen som sådan.

En uppgift som i och för sig utgör en abonnentuppgift kan även utgöra en trafikuppgift; det föreligger nämligen inget motsatsförhållande däremellan. Som exempel kan nämnas att telefonnummer typiskt sett är en abonnentuppgift, t.ex. när det återfinns i operatörens abonnentregister. När ett telefonnummer däremot finns registrerat såsom s.k. B-nummer (dvs. det mottagande numret i ett visst samtal mellan två personer över telefon) så utgör denna uppgift en trafikuppgift, eftersom det i denna situation är en teknisk uppgift som rör själva samtalet.

Till kategorin trafikuppgift räknas även lokaliseringsuppgifter, i den utsträckning det rör sig om sådana uppgifter avseende terminalutrustningens (dvs. mobiltelefonens) position som behandlas i mobilnätet och som är nödvändiga för överföringen av elektroniska meddelanden eller för att fakturera dessa. För att en lokaliseringsuppgift ska anses vara nödvändig för överföringen torde krävas att den rent tekniskt finns registrerad i mobilnätet för att kunna koppla upp överföring eller vidmakthålla en pågående överföring av information till eller från en mobiltelefon. Att en uppgift, som av sådana orsaker har registrerats i mobilnätet, används även i andra syften förändrar inte uppgiftens karaktär av trafikuppgift.

De lokaliseringsuppgifter som faller utanför definitionen av trafikuppgifter, hör till en egen kategori som är föremål för särskilda hanteringsregler. Till denna kategori hör t.ex. lokaliseringsuppgifter som är GPS-baserade.

#### Särskilda regler om behandlingen av trafikuppgifter

I normalfallet äger operatören rätt att behandla såväl abonnent- som trafikuppgifter för vissa ändamål. Vad gäller trafikuppgifter föreskrivs dock i 6 kap. 5-8 §§ vissa begränsningar i hur länge uppgifterna får behandlas och vad de får användas till.

När en trafikuppgift som avser en viss person inte längre behövs för överföring eller fakturering av ett elektroniskt meddelande, måste uppgiften utplånas eller avidentifieras. Regeln har dock vissa undantag. Bl.a. får trafikuppgifter behandlas när de behövs för abonnentfakturering och fakturering av samtrafik eller för att tillhandahålla vissa tjänster, under

förutsättning att abonnenten har samtyckt till denna behandling. Behandlingen av trafikuppgifter får endast utföras av den som fått i uppdrag av den som tillhandahåller en elektronisk kommunikationstjänst att sköta vissa särskilda uppgifter.

Dessa begränsningar för behandlingen av trafikuppgifter gäller inte i vissa särskilt angivna fall. Det rör sig om situationer där en myndighet eller domstol behöver tillgång uppgifterna för att lösa tvister, när uppgifterna rör kommunikation som omfattas av beslut om hemlig teleavlyssning och liknande åtgärder samt när uppgifterna behövs för att förhindra och avslöja obehörig användning av elektroniska kommunikationsnät eller -tjänster.

Särskilda regler om behandlingen av lokaliseringssuppgifter som inte utgör trafikuppgifter

I 6 kap. 9 § anges att lokaliseringssuppgifter som inte utgör trafikuppgifter (t.ex. GPS-baserade lokaliseringssuppgifter) och som rör användare som är fysiska personer eller abonnenter som huvudregel inte får behandlas. Behandling är endast tillåten om uppgifterna först anonymiseras alternativt efter att användaren eller abonnenten lämnat sitt samtycke till behandlingen. Behandlingen får då endast ske i den utsträckning och under den tid som är nödvändig för att tillhandahålla en tjänst där uppgifterna behövs och operatören är skyldig att först informera abonnenten om vilken typ av uppgifter som behandlas, ändamålet med behandlingen samt hur länge behandlingen kommer att pågå.

Bestämmelserna begränsar vem som har rätt att behandla uppgifter

I 6 kap. 17 § uppställs en särskild begränsning som gäller innehållet i elektroniska meddelanden och trafikuppgifter. Av bestämmelsen framgår att, som huvudregel, inga andra än berörda användare får behandla eller ta del av sådana uppgifter. Regeln hindrar dock inte sådan behandling som omfattas av de särskilda reglerna om trafikuppgifter, som redogjorts för ovan. Begränsningen gäller inte heller om minst en av de användare som deltar i kommunikationen lämnat sitt samtycke till behandlingen.

Samtliga uppgifter omfattas av tystnadsplikt

Enligt 6 kap. 20 § gäller som huvudregel tystnadsplikt för såväl uppgifter om som innehållet i de elektroniska meddelanden som förmedlas. Detta innebär att den som tagit del av sådana uppgifter inte obehörigen får föra dem vidare till

annan. I 6 kap. 22 § föreskrivs vissa undantag från tystnadsplikten, främst i förhållande till brottsutredande myndigheter.<sup>2</sup>

## 2.3 Personuppgiftslagen

Allmänt

PuL är huvudsakligen tillämplig på behandling av personuppgifter som helt eller delvis utförs digitalt (3 §). Lagen omfattar personuppgiftsbehandling som utförs av företag som är etablerade i Sverige (4 §).

Sedan den 1 januari 2007 finns två separata regelverk i PuL. Utöver de s.k. hanteringsreglerna, som anger under vilka förutsättningar behandling av personuppgifter i strukturerat material är tillåtet, har det kommit till en missbruksregel enligt vilken behandling av personuppgifter i ostrukturerat material är tillåten under förutsättning att den inte kränker den enskilde (5 a §).

Hanteringsreglerna

I lagen finns vissa grundläggande krav på den som behandlar personuppgifter, till exempel att personuppgifter bara får samlas in för särskilda uttryckligt angivna och berättigade ändamål. Uppgifterna får sedan inte användas för ändamål som är oförenliga med det ändamål för vilka uppgifterna samlades in och att uppgifterna inte får sparas under längre tid än vad som är nödvändigt med hänsyn till ändamålen (9 §). I PuL anges också när behandling av personuppgifter är tillåten. Utgångspunkten är att personuppgifter bara får behandlas om den registrerade har lämnat sitt samtycke till behandlingen (10 §). Utan samtycke får uppgifterna bara behandlas när behandlingen är nödvändig i vissa situationer till exempel om det är nödvändigt för att fullgöra ett avtal med den registrerade. Det kan också vara tillåtet att behandla personuppgifter med stöd av en s.k. intresseavvägning.

För känsliga personuppgifter gäller särskilda restriktioner (13-19 §§). Det är endast de uppgifter som anges 13 § PuL som är känsliga personuppgifter i PuL:s mening. Ett exempel på känsliga personuppgifter är uppgifter som rör hälsa eller sexualliv. Huvudregeln är att det är förbjudet att behandla känsliga personuppgifter om den registrerade inte har lämnat sitt uttryckliga samtycke till behandlingen.

PuL innehåller även regler om information till de registrerade (23-27 §§). Om den registrerades samtycke krävs för att behandlingen av hans eller hennes personuppgifter ska vara tillåten, måste samtycket alltid föregås av information. Även i de fall som personuppgifter behandlas med stöd av en annan grund än

---

<sup>2</sup> För mer information se information på PTS webbplats; [PTS sammanställning av praxis kring utlämnande av teleuppgifter](#).

Samtycke måste den personuppgiftsansvarige som huvudregel lämna information till den registrerade. Den registrerade har också rätt att en gång per kalenderår, efter en skriftligt undertecknad ansökan, få besked om vilka personuppgifter om honom eller henne som behandlas och hur uppgifterna behandlas (ett s.k. registerutdrag).

Den registrerade har rätt att på begäran få rättelse om personuppgifterna inte har behandlats i enlighet med bestämmelserna i PuL, det vill säga om uppgifterna är felaktiga eller om personuppgiftsbehandlingen på något annat sätt strider mot lagen (28 §).

I PuL finns även regler om säkerhet vid behandling av personuppgifter (30-32 §§). Mer information om detta lämnas i avsnittet om säkerhet.

Det är enligt huvudregeln förbjudet att föra över personuppgifter till tredje land (land utanför EU/EES) om landet inte har en adekvat skyddsnivå (33 §). Vilka länder som anses ha en adekvat skyddsnivå beslutas av EU-kommissionen. Förbudet gäller inte om t.ex. den registrerade lämnat sitt samtycke till överföringen eller om överföringen är nödvändig för att ett avtal mellan den registrerade och den personuppgiftsansvarige ska kunna fullgöras (34 §). Det kan också vara tillåtet enligt föreskrifter eller särskilda beslut av regeringen eller Datainspektionen, om det finns tillräckliga garantier för att de registrerades rättigheter skyddas. Sådana garantier kan finnas genom s.k. standardavtalsklausuler som EU-kommissionen godkänt eller genom bindande företagsinterna regler, Binding Corporate Rules – BCR (35 §).<sup>3</sup>

En personuppgiftsansvarig, till exempel ett företag, som behandlar personuppgifter i strid med PuL kan bli skadeståndsskyldig gentemot den registrerade (48 §). Lagen innehåller även bestämmelser om straff för den som bryter mot vissa bestämmelser i lagen, till exempel genom att lämna osann information till de registrerade (49 §).

#### Särskilt om samtycke

I personuppgiftslagen definieras ett samtycke som varje slag av *frivillig, särskild* och *otvetydig* viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne (3 §).

Att ett samtycke ska vara *frivilligt* innebär att den enskilde i praktiken måste ha ett fritt val att avgöra om hans eller hennes uppgifter ska få behandlas. I de

---

<sup>3</sup> För mer information om vad som gäller vid överföring av personuppgifter till tredje land, se [www.datainspektionen.se/om-oss/internationellt-arbete/tredjelandsoverforing/](http://www.datainspektionen.se/om-oss/internationellt-arbete/tredjelandsoverforing/).

flesta fall vållar inte kravet på frivillighet några bekymmer utan den enskilde får, efter att ha fått information om behandlingen, själv ta ställning till om han eller hon accepterar behandlingen för att till exempel erhålla en vara eller en tjänst.

Kravet på att samtycket ska vara *särskilt* innebär att ett generellt samtycke till behandling av personuppgifter inte godtas. Samtycket ska avse behandling för ett eller flera preciserade ändamål.

Att samtycket ska vara en *otvetydig* viljeyttring innebär att det inte får råda någon tvekan om att den registrerade godtar behandlingen av personuppgifter som rör honom eller henne. Det är den personuppgiftsansvarige som har bevisbördan för att samtycke faktiskt finns. Samtycket kräver inte viss form. Det behöver inte vara skriftligt utan kan lämnas muntligt, men skriftligt samtycke kan vara bra för att kunna visa att samtycke inhämtats.

För att samtycket ska vara giltigt enligt PuL, ska den registrerade även ha fått tillräcklig information om behandlingen. Mer om detta finns nedan under särskild rubrik.

Samtycket ska vara individuellt. Det ska således vara den registrerade som genom viljeyttringen godtar behandlingen av personuppgifter.

För att ett giltigt samtycke ska kunna lämnas krävs också att den registrerade är kapabel att förstå innebörden av samtycket. Den som är underårig (det vill säga under 18 år) kan lämna giltigt samtycke till en behandling om han eller hon kan förstå innebörden av samtycket. Något entydigt svar på frågan om även den underåriges vårdnadshavare måste lämna sitt samtycke för att behandlingen ska vara tillåten, kan inte ges. Det kan variera från fall till fall och bero på faktorer som ålder, uppgifternas art och ändamålet med behandlingen. Som tumregel gäller att den som fyllt 15 själv kan ta ställning till samtyckesfrågan.

Särskilt om information till den registrerade

När personuppgifter samlas in och behandlas måste de personer som registreras bli informerade om detta (23-25 §§). Dessutom måste det finnas möjlighet för de registrerade att ta del av de uppgifter som registrerats om dem (26 §).

Det är den personuppgiftsansvarige som ska se till att den registrerade får den information som krävs.

Informationen som ska lämnas ska vara tydlig och begriplig och omfatta (25 §):

- uppgifter om den som är personuppgiftsansvarig, till exempel namn, adress, telefonnummer och i förekommande fall organisationsnummer och e-postadress
- ändamålen med behandlingen, det vill säga varför personuppgifterna registreras och hur de ska användas
- övrig information som den registrerade behöver känna till, som exempelvis:
  - vilka typer av uppgifter som ska behandlas
  - till vilka företag eller andra organisationer (eller typer av dessa) som uppgifterna kan komma att lämnas ut
  - om den registrerade är skyldig att lämna uppgifter
  - att den registrerade har rätt att begära ett registerutdrag för att kunna kontrollera vilken information som finns registrerad om honom eller henne
  - att den personuppgiftsansvarige är skyldig att på begäran av den registrerade rätta uppgifter som är felaktiga, ofullständiga eller missvisande

Det finns undantag från regeln att den personuppgiftsansvarige självmant ska lämna information, bland annat kan regler om sekretess och tystnadsplikt begränsa skyldigheten att informera. Information behöver heller inte lämnas om sådant som den registrerade redan känner till.

När uppgifter samlas in från personen själv ska den personuppgiftsansvarige lämna informationen i samband med att uppgifterna samlas in. Informationen lämnas enklast på samma sätt som insamlandet sker.

Informationen ska lämnas till den registrerade. Under förutsättning att den registrerade själv kan förstå informationen gäller detta även om den registrerade har god man eller förvaltare eller är underårig (en tumregel när det gäller underåriga är att information normalt bör kunna lämnas till den som fyllt 15 år). Annars bör informationen lämnas till den gode mannen eller förvaltaren eller till den underåriges vårdnadshavare.

Den registrerade har, efter ansökan, rätt att en gång per år kostnadsfritt få ta del av de personuppgifter som finns registrerade om honom eller henne (s.k. registerutdrag). En ansökan om registerutdrag ska göras skriftligen och vara undertecknad av den sökande själv (26 §).

### 3 Användning av uppgifter i mobila innehållstjänster

#### Sammanfattning

---

Innehållstjänster för mobila kommunikationer är en marknad under framväxt. Utvecklingen av kraftfullare mobiltelefoner med större möjligheter för tredjepartstillverkare att tillhandahålla programvara samt större möjligheter att tekniskt sammanställa och överföra trafikuppgifter innebär att marknaden har potential att utvecklas än mer.

Marknaden består främst av tre parter:

- Operatörerna, som förfogar över trafikuppgifterna i sina respektive nät.
- Innehållsleverantörerna, som utvecklar tjänster där uppgifterna behövs, antingen som en del av tjänsten eller för att kunna fakturera tjänsten.
- Aggregatörerna, som utvecklat enhetliga gränssnitt för att effektivare möjliggöra överföring mellan innehållsleverantörer och operatörer.

Trots att marknaden är relativt ung finns idag en etablerad branschpraxis, uttryckt främst i de regler och rekommendationer som på ett tidigt stadium tagits fram och som löpande uppdateras, av branschorganisationerna MORGAN och Etiska rådet för betaltjänster.

#### 3.1 Allmänt om mobila innehållstjänster och dess leverantörer

Som konstaterats inledningsvis i denna rapport faller ett stort antal tjänster av varierande karaktär inom begreppet mobila innehållstjänster. ”Innehåll” är ett vagt och mycket omfattande begrepp som kan avse allt från en kort textmassa eller en ren betaltjänst till hela spelfilmer eller programvara. Operatörerna har i tillsynsenkäten uppgett att uppgifter lämnas till leverantörer av bl.a. ringsignaler, bilder, teman, chattar, dejting-, väder- och nyhetstjänster. Begreppet innehållstjänst tjänar därför i första hand syftet att dra en skiljelinje mot den underliggande kommunikationstjänsten, som tillhandahålls av en operatör.

Det är även svårt att definiera vad som gör en tjänst ”mobil”. Med hjälp av mer avancerade mobiltelefoner är det idag möjligt att i stor utsträckning tillgodogöra sig samma innehåll som via en vanlig persondator. Samtidigt blir datorerna i allt större utsträckning mobila och även försedda med teknik för uppkoppling mot mobilnäten. Många innehållstjänster bygger också på att användaren utför vissa åtgärder (t.ex. beställning) via en dator och att leveransen av innehållet (t.ex. en ringsignal) sker till en mobiltelefon. Även om utgångspunkten i denna rapport är användare som interagerar med innehållstjänster via en mobiltelefon är det dock huvudsakligen det faktum att denna kommunikation sker via mobilnät som är avgörande för resonemangen och slutsatserna som dras.

Leverantörerna av mobila innehållstjänster utgör en mycket heterogen grupp. På marknaden finns allt från de vars verksamhet bedrivs från hemmet, av en privatperson på dennes fritid, till internationella koncerner som omsätter stora belopp på distribution av t.ex. ringsignaler eller bakgrundsbilder. Det faktum att alla kontakter mellan leverantör och kund vanligen kan ske på elektronisk väg – allt från beställning till leverans av innehåll sker digitalt – ger dock även relativt små aktörer goda möjligheter att nå ut till kunder över hela världen. Flera av innehållsleverantörerna på den svenska marknaden saknar verksamhetsställe i Sverige. Detta faktum påverkar inte de principiella frågor som avhandlas i denna rapport men kan givetvis få praktisk betydelse för möjligheterna att upprätthålla efterlevnaden av tillämpliga bestämmelser.

Även om det har gått några år sedan de första mobila innehållstjänsterna etablerades torde marknaden ännu kunna sägas vara under framväxt. Tjänsternas komplexitet ökar och inte minst möjligheterna att använda positionering har skapat förutsättningar för nya, innovativa tjänster. I takt med att det blir allt vanligare med kraftfullare telefoner som även har öppna operativsystem, där nedladdning av programvara och annat innehåll som tillhandahålls av andra än telefon tillverkaren tillåts, följer även nya möjligheter till innehållstjänster.

Myndigheterna ser generellt positivt på en sådan utveckling. Samtidigt följer med ett ökat antal tjänster som nyttjar uppgifter om abonnenter och mobilanvändare, även ökad risk för intrång i den personliga integriteten.

### **3.2 Operatörers och aggregatörers roll på marknaden**

#### **Operatörer**

Flera av de svenska mobiloperatörerna tillhandahåller i varierande utsträckning egna innehållstjänster till sina abonnenter. Det kan röra sig om s.k. portaler, som fungerar som startsidor från vilka abonnenterna kan länkas vidare till

tjänster som tillhandahålls av externa leverantörer. I vissa fall erbjuds även mer omfattande innehållstjänster, gratis eller mot betalning.

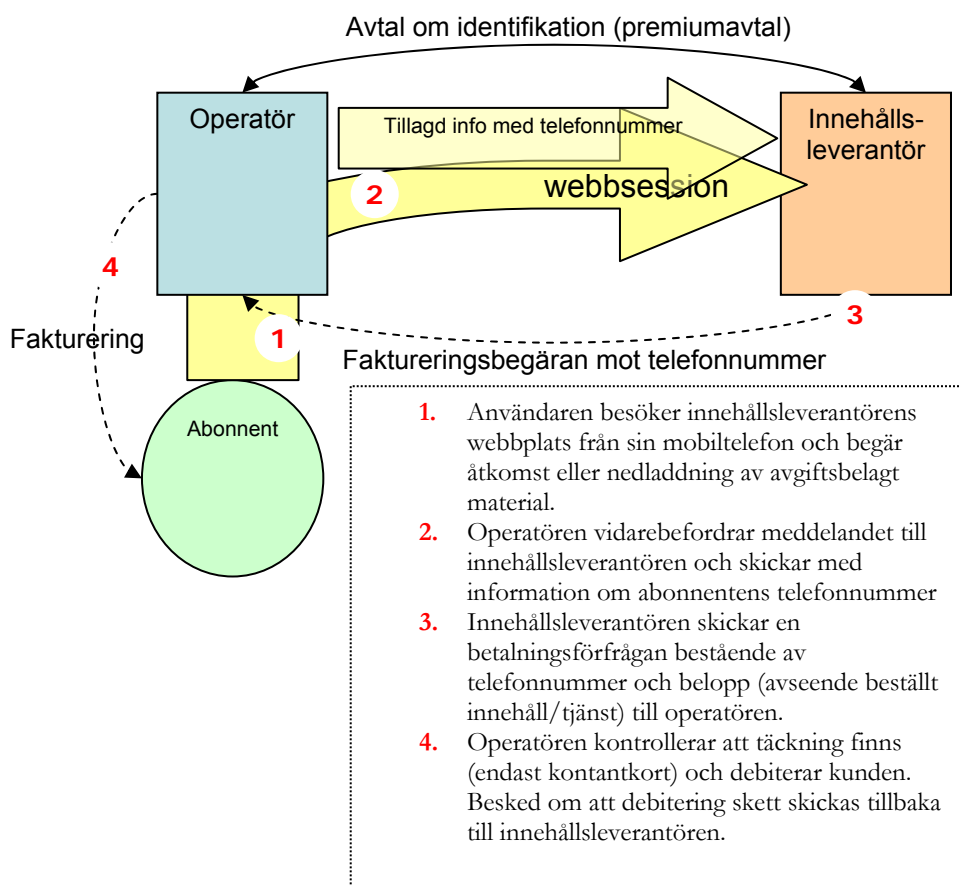
Av de uppgifter operatörerna lämnat framstår dock deras huvudsakliga roll vara som förmedlare av trafik mellan abonnenter och innehållsleverantörer. Utöver debitering för de meddelanden och den datatrafik som överförs, skapar det faktum att all trafik till och från en mobiltelefon passerar operatörens accesspunkt även möjligheter för denne att mot betalning förmedla uppgifter om abonnenten till innehållsleverantören. Det rör sig då huvudsakligen om identifieringsuppgifter i form av abonnentens telefonnummer, som överförs tillsammans med ett meddelande från abonnenten till innehållsleverantören.

I de fall meddelandet utgör ett sms eller mms så sker överföringen av telefonnumret genom traditionell nummerpresentation. När kommunikationen utgörs av webbtrafik, läggs uppgiften (telefonnumret) till i den begäran om en viss webbsida som överförs från abonnentens mobiltelefon till innehållsleverantörens webbserver. Uppgiften är i det senare fallet inte en teknisk förutsättning för att kommunikationen ska fungera, utan förmedlas för användning av innehållsleverantören.

I och med att operatören har en existerande kundrelation med abonnenten kan operatörerna även tillhandahålla en betalningslösning åt innehållsleverantörer, som innebär att kostnaden för de tjänster som beställs kan debiteras av operatören och läggas direkt på abonnentens telefonräkning eller, när det gäller kontantkort, dras från inestående saldo. För att utföra debitering skickar innehållsleverantören endast uppgift om telefonnummer och belopp till operatören. En schematisk beskrivning av förfarandet ges nedan i figur 1.

En fördel för innehållsleverantören med denna lösning är att betalning kan ske i realtid och utan att vare sig abonnenten eller innehållsleverantören behöver vidta några särskilda åtgärder för att säkerställa kundens identitet eller betalningsmedel. Detta bidrar i sin tur till att innehållstjänsten kan upplevas som enklare att nyttja för dess användare.

Figur 1 Flödet mellan abonnent, innehållsleverantör och operatör (vid åtkomst till wap-/webbaserad innehållstjänst)



### Aggregatörer

Det är i praktiken endast de största innehållsleverantörerna som direkt kommunicerar med varje enskild operatör. Mycket av kommunikationen mellan operatörer och innehållsleverantörer sker istället via en mellanhand, en s.k. aggregatör, som hanterar gränssnitten mellan innehållsleverantörerna och operatörerna. Samtliga operatörer uppger att uppgifter förmedlas såväl direkt till innehållsleverantörer som via aggregatörer.

I och med att aggregatörerna har avtal med samtliga operatörer och därmed kan förmedla uppgifter till och från dessa, slipper de innehållsleverantörer som använder sig av en aggregatörs tjänster teckna separata avtal med varje operatör och hantera varje operatörs tekniska gränssnitt, för att kunna erbjuda sina tjänster till samtliga mobilabbonenter. Det finns ett flertal fristående

aggregatörer men det förekommer även att mobiloperatörerna själva agerar aggregatör.

### 3.3 Användningen av lokaliseringssuppgifter

Uppgifter om mobilanvändares position används i allt större utsträckning i innehållstjänster. Det rör sig såväl om tjänster som är helt beroende av lokaliseringssuppgifter som tjänster där uppgifterna används för att skapa ett mervärde för användaren.

I takt med att allt fler mobiltelefoner förses med inbyggd GPS-mottagare ökar möjligheterna att använda den mycket precisa lokaliseringssuppgift som kan överföras direkt från telefonen till tjänsteleverantören. Detta kräver normalt en aktiv handling från användarens sida.

För att kunna lokalisera även användare som saknar GPS-mottagare i telefonen eller för att kunna utföra lokalisering utan att användaren aktivt skickar sin position, så krävs dock i regel att uppgifter om positionen lämnas av operatören.

Samtliga operatörer, som PTS har varit i kontakt med, har uppgett att uppgift om koordinat och osäkerhetsområde tillhandahålls. Uppgifterna utgår från vilken basstation eller cell som mobiltelefonen för tillfället kommunicerar med och en bedömning av på vilket avstånd från basstationen mobiltelefonen befinner sig. Osäkerhetsområdet är således en bedömning av inom vilket område en användare faktiskt befinner sig i. Finns det inom området många basstationer, som i tätorter, blir osäkerhetsområdet mindre och positionen därmed mer exakt.

Uppgifterna tillhandahålls av operatörerna via ett automatiserat gränssnitt som ursprungligen utvecklades för att kunna tillgodose SOS Alarms behov av att kunna positionera mobiltelefoner i samband med nödsamtal. Gränssnittet bygger på en svensk standard som arbetades fram i samarbete mellan SOS Alarm och de svenska operatörerna. Efter lanseringen för nödsamtalsändamål år 2006 har operatörerna kommersialiserat funktionen och erbjuder nu denna som en tjänst till innehållsleverantörer.

Förfarandet liknar det som redogjorts för ovan, avseende betalning. Innan positionering kan ske, måste innehållsleverantören fastställa användarens telefonnummer, vilket kan ske genom förmedling av operatören på det sätt som beskrivits ovan. Till skillnad från förmedling av abonnentens telefonnummer, som alltid skickas till innehållsleverantören (s.k. *push*-förfarande), så lämnas dock uppgift om position först på konkret förfrågan

från innehållsleverantören (s.k. *pull*-förfarande). En sådan förfrågan innehåller det telefonnummer som innehållsleverantören önskar positionera. Operatören utför positioneringen i realtid och svarar med användarens lokaliseringssuppgifter.

### 3.4 Aktörernas reglering av behandlingen

De lagstadgade regler som redogjorts för i föregående kapitel kompletteras av den reglering som marknadens aktörer själva har etablerat. Det rör sig främst om branschöverenskommelser och de individuella avtalen mellan operatörer, aggregatörer och innehållsleverantörer.

#### Branschöverenskommelser

Trots att marknaden är relativt ung finns idag en etablerad branschpraxis, uttryckt främst i de regler och rekommendationer som på ett tidigt stadium tagits fram och som löpande uppdateras, av branschorganisationerna MORGAN och Etiska rådet för betaltjänster.

Branschorganisationen MORGAN har utfärdat en s.k. *Code of Conduct*, som gäller vid distribution av mobila betalteletjänster och positionsbaserade tjänster i Sverige. Reglerna har tagits fram gemensamt av de svenska mobiloperatörerna och MORGAN. Av reglerna framgår att de är avsedda att följas av branschorganisationens medlemmar och att operatörerna i sina avtal med innehållsleverantörer ska ålägga dessa att följa reglerna.

*Code of Conduct* innehåller detaljerade regler för hur prenumeration på mobila innehållstjänster får startas och stoppas, hur och när betalning får ske liksom andra marknads- och konsumenträttsliga regler, gällande t.ex. innehållsleverantörernas kundtjänst och klagomålshantering.

Reglering gällande förmedling och annan behandling av personuppgifter saknas. För positionsbaserade tjänster finns dock regler av integritetsskyddande karaktär. Av reglerna framgår att sådana tjänster endast får aktiveras sedan innehållsleverantören inhämtat samtycke från abonnenten eller användaren. Separat samtycke ska inhämtas för varje specifik tjänst. För tjänster där det är uppenbart för beställaren att denne kommer att positioneras som en följd av beställningen gäller dock att beställningen av tjänsten i sig ska anses utgöra ett medgivande.

Flertalet av operatörerna uppger att *Code of Conduct* införlivats i avtalen med aggregatörer och innehållsleverantörer. Detta gör att reglerna i stor utsträckning är bindande mellan parterna på marknaden.

Etiska Rådet för Betalteletjänster har till uppgift att bl.a. utarbeta och upprätthålla etiska regler för innehållet i den information som lämnas på betalteletjänster och marknadsföringen av dessa.<sup>4</sup> De regler som rådet utfärdat omfattar dock inte aktörernas behandling av personuppgifter.

Avtalsförhållandet mellan operatörer och aggregatörer/innehållsleverantörer  
Operatörerna har kontroll över de uppgifter som behövs för att identifiera och positionera användare och har även en bestående kundrelation med abonnenten och möjlighet att debitera kundens telefonräkning eller kontantkortsaldo för beställda tjänster. De innehållsleverantörer som är i behov av sådana uppgifter eller av en sådan lösning för debitering av kunder, är därför beroende av ett avtal med operatörerna. Av denna orsak bestäms mycket av villkoren för förmedling av sådana uppgifter och betalningstjänster av operatörerna. Nedan redogörs för de uppgifter om dessa avtal som lämnats till PTS i operatörernas enkätsvar.

Samtliga operatörer förmedlar uppgifter såväl direkt till innehållsleverantörer som via aggregatörer. Operatörerna ställer i princip identiska krav på innehållsleverantörer och aggregatörer vad gäller villkor för behandling av uppgifterna, tekniska säkerhetsåtgärder, inhämtande av samtycke etc.

Dessa krav består i huvudsak av tre typer: Tekniska säkerhetskrav, krav på hur och när förmedlade uppgifter får hanteras samt krav på innehållsleverantörernas rutiner för information och beställning av innehållstjänster från användare.

Genomgående ställer operatörerna krav på att de uppgifter som förmedlas endast får användas i den utsträckning som krävs för att tillhandahålla innehållstjänsterna. Det förekommer även att operatörer förbehåller sig rätten att godkänna varje enskild tjänst som innehållsleverantörerna vill tillhandahålla. Behandlingen ska ske i enlighet med operatörens instruktioner och vanligen är aggregatörer och innehållsleverantörer skyldiga att utplåna samtliga uppgifter om operatörens abonnenter på dennes begäran. Avtalsregleringen gällande behandlingen av de förmedlade uppgifterna präglas i stor utsträckning av operatörernas behov av att kunduppgifter, som har ett stort affärsmässigt värde, inte kommer i orätta händer.

I viss utsträckning finns dock även reglering som specifikt relaterar till den regulatoriska aspekten av sådan behandling. Genomgående söker operatörerna

---

<sup>4</sup> Med betalteletjänster avses tjänster där den totala avgiften en konsument betalar till teleoperatören för tjänsten innefattar ersättning till tjänste- eller innehållsleverantör för tjänstens innehåll eller annan produkt eller tjänst levererad under uppkopplingen, eller som en direkt konsekvens av denna.

i detta avseende lägga ansvaret för behandlingen på respektive aggregatör och innehållsleverantör, för den faktiska behandling som sker hos dessa aktörer. Även i de fall operatören har uppgett att de anser aggregatörers och innehållsleverantörers behandling vara osjälvständig och utförd på operatörens uppdrag, framgår av avtalen att varje aktör ska bära ansvaret för behandlingen enligt LEK respektive PuL.

Avtalsförhållandet mellan aggregatörer och innehållsleverantörer

En av de fyra innehållsleverantörerna har uppgett att det inte förekommer att uppgifter förmedlas till dem från operatören via en aggregatör.

Genomgången av innehållsleverantörernas avtalsvillkor med kunden tyder på att innehållsleverantörerna anser sig vara personuppgiftsansvariga för den personuppgiftsbehandling som de utför. Det har vidare framkommit att aggregatörerna anser att innehållsleverantörerna är ansvariga för behandlingen av uppgifterna. Aggregatörerna kräver också att innehållsleverantörerna följer *MORGAN Code of Conduct*.

## 4 Bedömning av behandlingen av uppgifter för mobila innehållstjänster

### Sammanfattning

---

#### *Vilken lag är tillämplig?*

I de fall innehållstjänsten tillhandahålls på operatörens uppdrag och innehållsleverantören endast utgör en osjälvständig uppdragstagare (i denna rapport kallad "uppdragstjänst") är LEK tillämplig på samtliga parter behandling av uppgifterna.

I de fall innehållstjänsten inte tillhandahålls på uppdrag av operatören är LEK endast tillämplig på överföringen av uppgifterna från operatör till innehållsleverantör/aggregatör. Den vidare behandling som sedan sker av uppgifterna hos innehållsleverantörer och aggregatörer regleras av PuL.

#### *Kraven på samtycke*

Samtycke krävs enligt LEK för att överföra trafikuppgifter från operatören till utomstående part. Operatören ansvarar för att samtycke inhämtas innan överföring sker. Samtycke ska lämnas av abonnenten. Det finns inga formregler för hur ett samtycke ska inhämtas, utan det är upp till operatören att visa att så har skett.

När det inte är fråga om uppdragstjänster är innehållsleverantören personuppgiftsansvarig enligt PuL för den behandling som sker efter att uppgifter överförs från operatören. Utgångspunkten är att det krävs ett samtycke från den registrerade men behandlingen kan också vara tillåten om den är nödvändig för att avtalet med den registrerade ska kunna fullgöras eller efter en intresseavvägning.

I de fall operatören ansvarar för hela behandlingen (uppdragstjänster) krävs att samtycket som inhämtats av operatören omfattar även behandling av uppgifterna som sker i innehållstjänsten. När det gäller lokaliseringssuppgifter ska samtycket lämnas av den som använder mobiltelefonen.

Aggregatören utför endast behandling för innehållsleverantörens räkning och utgör därför ett s.k. personuppgiftsbiträde. Aggregatören behöver därför inte inhämta något eget samtycke, eftersom innehållsleverantören är ansvarig även för aggregatörens behandling.

I detta kapitel redogörs för myndigheternas bedömningar av hur reglerna i LEK och PuL bör tillämpas, när det gäller det utbyte av uppgifter som förekommer mellan operatörer, aggregatörer och innehållsleverantörer. Kapitel 4.1 har hållits kort och förhållandevis förenklat, en mer djupgående juridisk analys återfinns i bilaga 3.

I bilaga 4 finns även en schematisk bild över de frågor om tillämplig lag och samtyckeskrav som avhandlas i detta kapitel.

#### **4.1 Vilken lag ska tillämpas på behandlingen?**

Av de enkätsvar myndigheterna mottagit i tillsynen framgår att uppfattningen om vilken lagstiftning som är tillämplig skiftar mellan olika aktörer. Detta innebär att uppfattningen skiftar, också om vem som är ytterst ansvarig för behandlingen av uppgifterna, något som är olyckligt eftersom det riskerar att leda till en situation där ingen enskild aktör tar detta ansvar. Det finns två lagstiftningar – PuL och LEK – som kan vara tillämpliga på olika delar av hanteringen av trafikuppgifter. Detta kan givetvis leda till komplicerade bedömningar av när den ena ska gälla före den andra.

Myndigheternas slutsats är att det huvudsakligen finns två gränsdragningar mellan LEK och PuL: antingen är LEK tillämplig på all behandling av trafikuppgifter som samtliga aktörer vidtar eller så är LEK endast tillämplig på behandlingen som består av att uppgifterna överförs från operatörer till aggregatör/innehållsleverantör.

I de fall trafikuppgifter behandlas av innehållsleverantörer på uppdrag av operatören är LEK tillämplig på hela hanteringen. Uttrycket ”på uppdrag” tolkas snävt, vilket innebär att endast sådana situationer omfattas, där en operatör lejt ut viss del av verksamheten till en annan part som osjälvständigt utför denna. För att innehållsleverantören ska anses tillhandahålla en tjänst på uppdrag av en operatör, ska således tjänsten tillhandahållas i en av operatören kontrollerad form och i operatörens namn eller varumärke, så att det för användaren framstår som att det är operatören själv som tillhandahåller innehållstjänsten. Typfallet är en av operatören kontrollerad portal, där det för användaren aldrig framgår att tjänsterna levereras av andra än operatören. I denna rapport refereras denna form av innehållstjänst som ”uppdragstjänst”.

I de fall innehållstjänsten *inte* tillhandahålls på uppdrag av operatören är LEK endast tillämpligt på överföringen av uppgifterna från operatör till innehållsleverantör/aggregatör. Den vidare behandling som sedan sker av uppgifterna hos innehållsleverantörer och aggregatörer regleras av PuL.

Så som myndigheterna har uppfattat det, levereras merparten av de innehållstjänster som återfinns på marknaden idag av en fristående part, som för användaren ger ett relativt självständigt intryck. I dessa fall är det således inte tal om en uppdragstjänst.

Slutsatsen är därför att i de flesta fall är LEKs bestämmelser tillämpliga på operatörers överföring av telefonnummer (identifieringssyfte) och lokaliseringssuppgifter (lokaliseringssyfte) medan huvudregeln är att PuL blir tillämplig på innehållsleverantörers och eventuella aggregatörers vidare behandling av dessa uppgifter.

Av de svar operatörerna har lämnat i den genomförda tillsynsenkäten framgår att några operatörer anser att innehållsleverantörer generellt agerar på uppdrag av operatören medan andra operatörer anser att innehållsleverantörerna generellt utför en självständig behandling av uppgifterna som lämnas ut. Av svaren framgår inte om operatörerna gjort olika bedömningar i detta avseende, beroende på hur en viss innehållstjänst tillhandahålls eller marknadsförs. Myndigheternas slutsats i gränsdragningsfrågan kan utgöra skäl för operatörerna att se över ansvarsförhållandena, med utgångspunkt i en bedömning av om innehållstjänsterna utgör uppdragstjänster eller inte, se vidare kapitel 6.1.3.

I kapitlet nedan redovisas vad denna gränsdragningsfråga innebär när det gäller krav på att inhämta samtycke och villkor som följer av respektive lagstiftning.

#### **4.2 Vem ansvarar för att bestämmelserna i PuL följs?**

Det intryck Datainspektionen fått av de enkätsvar som innehållsleverantörer och aggregatörer lämnat, är att den uppgiftsbehandling som sker i de granskade mobila innehållstjänsterna initieras genom att användaren beställer en tjänst hos innehållsleverantörerna. De granskade innehållstjänsterna är alltså inte vad vi ovan kallat uppdragstjänster. Det är innehållsleverantörerna som bestämmer ändamålen med och medlen för den behandling som utförs inom ramen för tjänsten.

Myndigheten anser därför att innehållsleverantören ska vara att betrakta som personuppgiftsansvarig i personuppgiftslagens mening. Det är den personuppgiftsansvarige som är ansvarig för att bestämmelserna i PuL följs.

De aggregatörer som innehållsleverantören använder sig av, för att inhämta sådana uppgifter från operatören som behövs för att kunna leverera tjänsten, utför en behandling för innehållsleverantörens räkning. Det betyder att

aggregatören i dessa situationer är ett så kallat personuppgiftsbiträde och att innehållsleverantören är ansvarig även för dennes behandling.

Om ett personuppgiftsbiträde behandlar de aktuella personuppgifterna för helt andra ändamål än de den personuppgiftsansvarige bestämt, har den personuppgiftsansvarige ansvaret för att så har kunnat ske, t.ex. för brister i säkerheten eller givna instruktioner. Den som påbörjar en behandling för nya ändamål kan i sin tur blir personuppgiftsansvarig för sin vidare behandling.

### **4.3 När krävs samtycke för att behandlingen ska vara tillåten?**

Med utgångspunkt i den bedömning som gjorts ovan, avseende vilken lag som ska tillämpas på de olika delarna av överföringen av trafikuppgifter, kan en bedömning göras av när ett samtycke måste inhämtas från abonnenten eller användaren, för att behandlingen ska anses tillåten. Det bör i sammanhanget påpekas att i den mån krav på samtycke föreligger enligt LEK, närmare bedömningar avseende vad som utgör ett giltigt samtycke, hur och av vem det ska inhämtas m.m. ska göras i enlighet med reglerna i PuL (dessa beskrivs ovan i kapitel 2.3). Vidare bör påpekas att även när en behandling som omfattas av PuL stödjer sig på ett samtycke så måste övriga bestämmelser i PuL vara uppfyllda för att behandlingen ska anses laglig.

Det bör också tilläggas att de slutsatser som redovisas i följande avsnitt är generella slutsatser utifrån den information om utbytet av uppgifter som myndigheterna fått från marknadens aktörer, genom sina respektive tillsynsenkäter. Syftet med nedanstående avsnitt är inte att i enskilda fall bedöma huruvida aktörerna uppfyller lagen eller inte, utan att belysa de krav som ställs.

#### **4.3.1 Operatörer**

Krävs samtycke för operatörens behandling?

Som har beskrivits ovan är det myndigheternas bedömning att LEK generellt gäller för behandling i form av utlämning av trafikuppgifter från operatör till utomstående part. När det gäller den utomstående partens vidare behandling av trafikuppgiften ska denna behandling i normalfallet bedömas utifrån PuL.

Eftersom det inte finns några möjligheter till undantag från samtyckeskravet genom intresseavvägningar eller annat i LEK, krävs samtycke för utlämnande av trafikuppgifter. Detta gäller såväl de trafikuppgifter som utlämnas i identifikationssyfte som lokaliseringssyfte.

När det gäller uppdragstjänster, där operatören ansvarar för hela behandlingen, ska samtycket omfatta både den behandling som operatören själv vidtar och den som utförs av uppdragstagare.

Samtliga operatörer har uppgett att de inhämtar samtycke både för den behandling de själva utför och för utlämnandet av uppgifter till aggregatörer och innehållsleverantörer. Av operatörernas svar framgår dock inte tydligt i vilken utsträckning det samtycke som inhämtas också omfattar den behandling som utförs av innehållsleverantörer (vilket alltså är nödvändigt när det gäller uppdragstjänster).

Vem kan inhämta ett samtycke?

En fråga i sammanhanget är vilken aktör som ska inhämta samtycket. En utgångspunkt i PuL är att den personuppgiftsansvarige är ansvarig för att personuppgifterna behandlas i enlighet med lagen och således även att samtycke införskaffas, för det fall så krävs. Operatören ansvarar alltså för att samtycke inhämtas, när det gäller den behandling som operatören ansvarar för. Detta innebär inte nödvändigtvis att det är operatören som de facto måste inhämta samtycket, utan det kan mycket väl ske av annan aktör som i avtal med operatören har åtagit sig detta. Det är dock viktigt att påpeka att den som är ansvarig i lagens mening alltid är den som ansvarar för att kraven uppfylls och att det därmed också är denne som skadeståndsanspråk och i vissa fall även straff kan riktas mot, om lagens skyldigheter inte upprätthålls. Det ligger därför i operatörens intresse att säkerställa att korrekta samtycken verkligen inhämtas.

Hur ska samtycke inhämtas

I PuL definieras ett samtycke som varje slag av *frivillig, särskild och otvetydig* viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne.

Det framgår av de enkätsvar som inkommit att merparten av operatörerna använder sig av samtycken som införts i det generella avtalet om abonnemang, vilket kan te sig naturligt då detta avtal innehåller de villkor som gäller mellan abonnent och operatör. Det finns inga formregler för hur samtycket ska inhämtas och ett samtycke kan därför mycket väl återfinnas i det allmänna avtalet kring abonnemanget. Eftersom samtycket ska vara *särskilt* räcker det inte med ett generellt samtycke till behandling av personuppgifter, utan ändamålet måste preciseras. Det är operatören som är ansvarig för att samtycke faktiskt finns och denne har därmed också bevisbördan för att samtycket inhämtats.

Det är enligt LEK inte möjligt att ”ärva ett samtycke”. Det innebär att aggregatörer och innehållsleverantörer, i de fall PuL ställer krav på samtycke för den behandling som dessa aktörer utför (se vidare angående detta nedan i kapitlen 4.3.2 och 4.3.3), inte kan förlita sig på ett samtycke som operatören redan har inhämtat. Detta utesluter förvisso inte att en aggregatör eller innehållsleverantör tar hjälp av operatören eller någon annan med att inhämta samtycke, men detta innebär inte att ansvaret för att samtycke inhämtas förskjuts.

Vem kan ge ett samtycke?

En annan fråga är vem som ska ge samtycket. Abonnten är inte nödvändigtvis en fysisk person eller samma fysiska person som den som använder mobiltelefonen eller abonnemanget. Inom t.ex. en familj eller ett företag, kan ett flertal olika fysiska personer använda samma abonnemang.

Enligt förarbetena ska utgångspunkten i enlighet med PuL vara att den som samtycker också ska vara den fysiska person vars personuppgifter behandlas.<sup>5</sup> Eftersom trafikuppgifter inte behöver utgöra personuppgifter blir dock ledningen något haltande, men lagstiftarens mening torde vara att utgångspunkten alltid ska vara den fysiska person som trafikuppgifterna rör. I punkten 31 i preambeln till direktivet om integritet och elektronisk kommunikation anges att avgörandet huruvida det är användaren (dvs. den person som nyttjar tjänsten) eller abonnenten (dvs. den som har ingått avtalet om abonnemang) som ska ge sitt samtycke till behandlingen av personuppgifter ”beror på vilken typ av uppgift som ska behandlas, vilken tjänst som erbjuds och om det är tekniskt, formellt och avtalsmässigt möjligt att skilja mellan en enskild persons användning av en elektronisk kommunikationstjänst och den juridiska eller fysiska person som abonnerat på den.” Att man i denna punkt i preambeln nämner personuppgifter i motsats till trafikuppgifter är något förvånande då begreppet mervärdestjänst definieras som ”alla tjänster som kräver behandling av trafik- eller lokaliseringssuppgifter utöver vad som är nödvändigt för överföring eller fakturering av en kommunikation.”<sup>6</sup>

Mot bakgrund av uttalanden i förarbetena är det en rimlig slutsats att även om utgångspunkten alltid ska vara att den fysiska person som uppgifterna berör också ska vara den som samtycker till behandlingen är detta trots allt en utgångspunkt som inte alltid strikt kan tillämpas. Även om samtycke ska ges samma betydelse som i PuL, där det alltid är den som personuppgifterna berör som ska ge samtycket, säger det sig själv att detta inte strikt går att tillämpa på

---

<sup>5</sup> Prop 2002/03:110, sid 258

<sup>6</sup> Se art 2 punkten g), direktiv 2002/58/EG om integritet och elektronisk kommunikation

trafikuppgifter som inte självklart berör en viss fysisk person. Utgångspunkten bör dock vara att det är den som trafikuppgifterna berör vid tillfället för användning av innehållstjänsten som ska samtycka till behandlingen.

Vid överföring av uppgifter till en innehållsleverantör är det PTS uppfattning att det normalt är tillräckligt att abonnenten är den som samtycker till att de aktuella uppgifterna *överförs* från operatören för användning i innehållstjänster eftersom det främst är abonnenten som berörs av dessa uppgifter. Innehållsleverantören ansvarar normalt för den vidare användningen av uppgifterna i innehållstjänsten och, i den mån denna behandling kräver samtycke, för inhämtande av detta, i enlighet med PuL.

När det gäller *uppdragstjänster* ansvarar däremot operatören för hela behandlingen enligt LEK, varför operatören måste inhämta samtycke från den som berörs av den faktiska användningen av uppgifterna. Vid användning av uppgifter i lokaliseringssyfte är det således PTS uppfattning att det är användaren (som förvisso i de flesta fall torde vara densamme som abonnenten) som måste samtycka till överföringen, eftersom uppgifterna är direkt hänförliga till var denne befinner sig för tillfället. Sådant samtycke bör således ges i samband med att tjänsten tillhandahålls. Vid identifieringssyfte är det däremot myndighetens uppfattning att det är tillräckligt med att abonnenten samtyckt till denna användning, eftersom syftet med behandlingen är att säkerställa just abonnentens identitet, och sådant samtycke kan således återfinnas i abonnemangsavtalet.

Flertalet operatörer uppger att samtycke inhämtas från abonnenten. I något fall påpekar operatören abonnent och användare i deras mening är samme person eftersom samtliga rättigheter och skyldigheter enligt abonnemangsavtalet är knutna till abonnenten. I MORGANs *Code of Conduct* anges, när det gäller samtycke till positionering, att detta ska inhämtas från ”abbonenten eller användaren”, vilket antyder att man förvisso gör skillnad mellan de två, men att det är egalt från vem samtycke inhämtas. Det bör dock påpekas att en av operatörerna uppger att samtycke alltid hämtas från användaren eftersom det är denne som håller i telefonen.

Mot bakgrund av PTS bedömningar ovan, kan det finnas anledning för operatörerna att se över rutinerna för inhämtande av samtycke, se vidare kapitel 6.1.3.

### 4.3.2 Innehållsleverantören

Krävs samtycke för innehållsleverantörens behandling?

Även enligt personuppgiftslagen är utgångspunkten att det krävs ett *samtycke* från den registrerade för att personuppgifter ska få behandlas. För information om vad som krävs för ett giltigt samtycke se kapitel 2.3. En alternativ grund för behandlingen är om behandlingen är *nödvändig* för att ett avtal med den registrerade ska kunna fullgöras. En annan alternativ grund för behandlingen kan vara den s.k. intresseavvägningen.

Innehållsleverantörer kan alltid välja att stödja sin behandling, av alla de personuppgifter de behandlar, på samtycke från den registrerade. I tillsynen mot innehållsleverantörerna har samtliga svarat att grunden för deras behandling av uppgifter i innehållstjänsten är samtycke. För att samtycket ska vara giltigt krävs bl.a. att den registrerade har fått tillräcklig information om den tilltänkta behandlingen. Den information som de granskade innehållsleverantörerna ger är dock inte alltid tillräckligt tydlig för att den ska kunna ligga till grund för ett giltigt samtycke. Ändamålen med behandlingen är ibland ottydligt beskrivna och i vissa fall saknas uttömmande information om vilka personuppgifter som kommer att behandlas. Som framgår ovan kan dock behandling som är nödvändig för den mobila innehållstjänsten stödjas på avtalet med den registrerade (kunden), även om avtalet inte innehåller ett uttryckligt samtycke. Men även då behandlingen inte sker med stöd av samtycke har innehållsleverantörerna krav på sig att lämna information till de registrerade (se kapitel 2.3).

Vid sådan behandling som utförs i samband med tillhandahållandet av lokaliseringstjänster är det Datainspektionens uppfattning att behandlingen av *lokaliseringssuppgifter* kan ske med stöd av avtalet som träffas mellan innehållsleverantören och den registrerade, eftersom denna behandling är nödvändig för att kunna leverera den beställda tjänsten. Detta under förutsättning att det står klart för användaren att lokaliseringssuppgifter används, som t.ex. i tjänster av typen ”hitta närmaste restaurang”. Detta synsätt överrensstämmer med vad som framkommer i MORGANs branschregler avseende krav på inhämtande av samtycke.

Även innehållsleverantörens behandling av *telefonnummer* kan ske med stöd av avtalet som träffas mellan innehållsleverantören och den registrerade. Det är dock bara i de fall då behandlingen är *nödvändig* för att avtalet ska kunna fullgöras. Behandlingen kan t.ex. vara tillåten om den är nödvändig för att innehållsleverantören ska kunna ta betalt av användaren, t.ex. vid betalning via SMS eller vid webbsessioner där användaren beställer material. Behandlingen förutsätter dock att det står klart för användaren att telefonnumret används.

Vem ska inhämta samtycke?

Det är *innehållsleverantören*, i de fall samtycke krävs, som är ansvarig för att inhämta samtycke för sin egen behandling och för den behandling som aggregatörer utför på uppdrag av dem, eftersom det är innehållsleverantören som är personuppgiftsansvarig. Att det är innehållsleverantören som ska inhämta samtycke har också nedtecknats i MORGANs branschregler om krav på inhämtande av samtycke.

Hur ska samtycke inhämtas?

Det finns inget krav på hur ett samtycke ska inhämtas. Vid användning av mobila innehållstjänster kan det dock ofta vara lämpligt att inhämta samtycke via mobilen.

Vem kan ge ett samtycke?

Enligt PuL är det den registrerade, den vars uppgifter som behandlas, som ska samtycka till behandlingen. I de allra flesta fall torde den registrerade vara densamme som abonnenten. Den som är minst 15 år får anses kunna lämna ett sådant giltigt samtycke som krävs vid användning av mobila innehållstjänster.

#### **4.3.3 Aggregatören**

Som nämnts i avsnittet ovan är det den personuppgiftsansvarige, dvs. innehållsleverantören, som är skyldig att se till att ett giltigt samtycke inhämtas.

Eftersom aggregatören snarast är personuppgiftsbiträde till innehållsleverantören behöver aggregatören inte inhämta något samtycke för den behandling den utför för innehållsleverantörens räkning.

Om aggregatören däremot på något sätt behandlar uppgifter självständigt måste aggregatören givetvis inhämta ett samtycke i de fall ett sådant krävs. På samma sätt som ett samtycke inte kan ”ärvas” enligt LEK kan det heller inte ”ärvas” enligt PuL. Med hänsyn till att aggregatören agerar som mellanhand till operatörer och innehållsleverantörer och inte har någon direktkontakt med användare, kan det vara svårt för aggregatören att själv inhämta ett samtycke för den självständiga behandlingen. I sådana fall måste aggregatören ta hjälp av operatören eller innehållsleverantören för inhämtande av samtycke.

#### **4.4 Uppfylls övriga krav på behandlingen?**

I det här avsnittet analyseras i vad mån innehållsleverantörernas behandling av personuppgifter kan anses förenlig med de krav som PuL i övrigt ställer på behandlingen. Eftersom det är innehållsleverantören som är personuppgiftsansvarig ansvarar den även för att aggregatörens behandling är förenlig med PuL. Aggregatörernas behandling kommer därför inte att

behandlas i detta avsnitt. (För det fall att aggregatören behandlar uppgifter självständigt och behandlingen omfattas av PuL måste givetvis även aggregatören uppfylla PuLs bestämmelser.)

Inte heller kommer operatörens behandling tas upp i detta avsnitt eftersom dennes behandling, enligt slutsatserna ovan, alltid omfattas av bestämmelserna i LEK. I viss utsträckning innehåller LEK bestämmelser som motsvarar de som redogörs för i detta avsnitt. Med undantag för bestämmelsen om säkerhetsåtgärder har PTS emellertid inte utrett frågan om sådana bestämmelser efterlevs, inom ramen för den genomförda tillsynen.

#### Grundläggande krav

Enligt de grundläggande kraven i PuL får personuppgifter endast användas för förutbestämda ändamål. Uppgifterna får sedan inte användas för ändamål som är oförenliga med det ändamål för vilka uppgifterna samlades in. Om syftet med en erbjuden tjänst är att tala om för användaren var t.ex. närmaste restaurang finns, är det inte tillåtet att använda lokaliseringssuppgifterna för andra ändamål, t.ex. för att meddela en restaurang om vilka som befinner sig i närheten av restaurangen. En sådan ändamålsglidning är aldrig tillåten. Granskningen av innehållsleverantörerna har dock inte visat annat är att de insamlade uppgifterna används endast för att leverera de beställda innehållstjänsterna.

De uppgifter som används för tillhandahållande av de granskade innehållstjänsterna är framförallt lokaliseringssuppgifter (för lokaliseringssyfte) och telefonnummer (för identifieringssyfte).

Behandlingen av lokaliseringssuppgifter måste anses adekvat och relevant vid tillhandahållande av lokaliseringstjänster. Det är en förutsättning för att kunna leverera den beställda tjänsten att sådana uppgifter behandlas.

Ett av de bakomliggande skälen till denna granskning är den information som myndigheterna fått genom uppgifter i media om att mobiltelefonanvändare som använder Internet i sin mobil ovetandes får sitt telefonnummer utlämnat till de webbplatser/innehållsleverantörer som de besöker. Ingen av de granskade innehållsleverantörerna har uppgett att man får information om mobilinnehavarens telefonnummer på detta sätt. För det fall denna information regelmässigt lämnas till innehållsleverantörer, utan att användaren beställt någon tjänst, gör Datainspektionen bedömningen att mycket talar för att sådan behandling innebär att uppgifter behandlas i strid med de grundläggande kraven i 9 § PuL. En annan sak är om mobilinnehavaren använder Internet i mobilen för att beställa t.ex. ringsignaler eller andra tjänster

från en innehållsleverantör. Då kan det vara så att uppgifterna är adekvata och relevanta och att behandlingen av uppgifterna är nödvändig för att kunna fakturera och/eller leverera beställt material till mobilinnehavaren, vilket gör att behandlingen är tillåten. Under avsnittet om rekommendationer, kap 6, tas dock frågan upp om det går att använda en annan uppgift än mobilinnehavarens telefonnummer för identifiering och fakturering.

Det har även framkommit att innehållsleverantörerna samlar in andra personuppgifter, t.ex. namn och adress, genom ett registreringsförfarande via webbplats. Hanteringen av uppgifter som inhämtas vid registreringsförfarandet ligger dock utanför fokus för denna rapport avseende mobila innehållstjänster, men givetvis måste PuLs bestämmelser följas även vid behandling av dessa uppgifter.

Det har inte framkommit hur länge innehållsleverantörerna sparar de insamlade uppgifterna. Datainspektionen vill understryka att uppgifterna inte får sparas längre än vad som är nödvändigt med hänsyn till ändamålet för behandlingen, dvs. för att tillhandahålla den mobila innehållstjänsten. För innehållsleverantörer, och därmed också aggregatörer, är det knappast aktuellt att spara uppgifterna annat än en mycket kort tidsperiod.

#### Information

En av förutsättningarna för att en behandling ska vara tillåten enligt PuL är att den registrerade har fått tillräcklig information. Det är särskilt viktigt att informationen är tydlig vid inhämtande av samtycke, eftersom samtycket annars inte kan anses giltigt. Men även när samtycke inte inhämtas måste innehållsleverantörerna lämna information om: den personuppgiftsansvariges identitet, ändamålen med behandlingen, vilka uppgifter som behandlas, till vem eller vilka företag som uppgifterna kan komma att lämnas ut, om den registrerade är skyldig att lämna uppgifter, rätten att ansöka om s.k. registerutdrag och möjligheten att få rättelse. Information behöver inte lämnas om sådant som den registrerade redan känner till.

De innehållsleverantörer Datainspektionen har granskat har hänvisat till att de lämnar skriftlig information till de registrerade (kallad användarvillkor, integritetspolicy eller information till de registrerade). I samband med granskningen har Datainspektionen sett att informationen som innehållsleverantörerna lämnar kan förbättras i flera avseenden. Framförallt gäller det information om rätten till registerutdrag och möjligheten att begära rättelse. I vissa fall gäller det även uppgift om den personuppgiftsansvariges identitet och kontaktuppgifter. Ändamålen med behandlingen är ibland ottydligt beskriven och i vissa fall saknas uttömmande information om vilka uppgifter

som kommer att behandlas. Så länge den registrerade själv lämnar uppgifterna till innehållsleverantören får den registrerade dock förutsättas känna till att uppgiften kommer att behandlas.

#### Säkerhetsåtgärder – Biträdesavtal

Se nedan under kapitel 5.1 om säkerhet.

#### Överföring till tredje land

Vid den genomförda granskningen har fokus inte legat på om innehållsleverantörerna överför några uppgifter till tredje land (land utanför EU/EES). Datainspektionen vill ändå i det här sammanhanget påminna om att de innehållsleverantörer som skickar uppgifter till någon i tredje land eller som använder sig av en egen server i tredje land måste följa bestämmelserna i 33-35 §§ PuL.

## 5 Säkerheten vid överföring av uppgifter

### Sammanfattning

---

Både operatörer (enligt LEK) och innehållsleverantörer (enligt PuL) är skyldiga att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de uppgifter som behandlas.

Datainspektionen har tagit fram allmänna råd för säkerhet vid behandling av personuppgifter och det finns även en svensk standard för informationssäkerhet.

De grundläggande principerna för att skydda uppgifter är autentisering, auktorisation, konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Överföringen av trafikuppgifter mellan operatörer, aggregatörer och innehållsleverantörer skyddas dels av inbyggda skyddsmekanismer i mobilnäten, dels av skyddsåtgärder som aktörerna vidtagit i form av t.ex. kryptering av informationen. Tillgången till operatörernas system för debitering eller positionering av abonnenter skyddas vanligen också genom olika autentiseringsförfaranden.

Ovan har redogjorts för de krav som LEK och PuL ställer på aktörerna, när det gäller inhämtande av samtycke, information till den registrerade m.m. I både LEK och PuL finns även bestämmelser om att den som tillhandahåller allmänt tillgängliga kommunikationstjänster och nät respektive den som behandlar personuppgifter, ska vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Med skydd menas att upprätthålla informationssäkerhet och att hantera det som *inte* ska hända, dvs. att hantera hot i informationssystem. Det gäller både vid överföring och vid lagring.

I det här kapitlet presenteras inledningsvis kort de grundläggande principer som bör tillämpas för att upprätthålla informationssäkerhet i informationssystem. Därefter redogörs för de tekniker som är vanligt tillämpade för överföring av uppgifter i tillhandahållandet av mobila innehållstjänster och vilket skydd de medför samt hur överföring av uppgifter sker mellan operatörer, aggregatörer och innehållsleverantörer för att realisera

mobila innehållstjänster utifrån de uppgifter som lämnats av aktörerna inom den tillsyn som myndigheterna har genomfört. Myndigheternas rekommendationer beträffande skydd av uppgifter återfinns i kapitel 6.2.

### **5.1 Regleringen om skydd av uppgifter i mobila innehållstjänster**

Operatörer ska, enligt LEK, vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas (6 kap. 3 §). Vidare ska den som tillhandahåller ett allmänt kommunikationsnät, dvs. operatören, vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå, som med beaktande av tillgänglig teknik och kostnader för att genomföra åtgärderna, är anpassad till risken för integritetsintrång.

Även PuL ställer krav på säkerhetsåtgärder. I PuL anges att den *personuppgiftsansvarige* ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas (31 §). Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av:

- de tekniska möjligheter som finns,
- vad det skulle kosta att genomföra åtgärderna,
- de särskilda risker som finns med behandlingen av personuppgifterna, och
- hur pass känsliga de behandlade personuppgifterna är.

Ju känsligare personuppgifterna är och ju större riskerna är med behandlingen av personuppgifterna, desto mer omfattande bör säkerhetsåtgärderna vara. Även mängden av uppgifter om varje person måste beaktas eftersom den bestämmer hur detaljerad bild det går att skapa om en person.

Som nyss nämnts ligger ansvaret på att det finns lämpliga säkerhetsåtgärder på den personuppgiftsansvarige. Den personuppgiftsansvarige kan välja att anlita ett personuppgiftsbiträde. Den personuppgiftsansvarige kan överlåta den faktiska behandlingen av personuppgifter, men ansvaret kan aldrig överlåtas. Det är alltid den personuppgiftsansvarige som ytterst svarar för att personuppgiftslagen följs och att de registrerade behandlas korrekt.

Som framgått i kapitel 4.1 är slutsatsen att det är innehållsleverantören som bestämmer ändamålen med och medlen för den behandling som utförs inom ramen för innehållstjänsterna, med undantag för en s.k. uppdragstjänst där behandlingen sker på uppdrag av operatören. Innehållsleverantören är därför att betrakta som personuppgiftsansvarig i personuppgiftslagens mening och

därmed också ansvarig för att bestämmelserna i PuL följs. De aggregatörer som innehållsleverantören använder sig av, för att inhämta sådana uppgifter från operatören som behövs för att kunna leverera tjänsten, utför en behandling för innehållsleverantörens räkning. Aggregatörerna agerar därför som personuppgiftsbiträden åt innehållsleverantörerna.

Om den personuppgiftsansvarige väljer att anlita ett personuppgiftsbiträde måste ett skriftligt avtal upprättas (30 §). Av avtalet ska det framgå att personuppgiftsbiträdet bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de säkerhetsåtgärder som framgår av 31 §. Kravet på skriftlighet innebär att avtalet måste vara uttryckt i text, men texten kan finnas på papper eller i elektronisk form. Något krav på att avtalet måste vara undertecknat finns inte, men det kan rekommenderas ur bevishänseende.

Utöver avtalet måste den personuppgiftsansvarige förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

Säkerhetsbestämmelsen i LEK tolkas på samma sätt som säkerhetsbestämmelsen i PuL. Det innebär att det inte är någon skillnad på de krav som ställs i respektive lag på säkerheten. LEK saknar dock ett liknande krav på skriftligt avtal som anges i PuL när den personuppgiftsansvarige anlitar ett personuppgiftsbiträde.

Datainspektionen har tagit fram allmänna råd gällande säkerhet vid behandling av personuppgifter, ”Säkerhet för personuppgifter”.

Utöver Datainspektionens allmänna råd om säkerhet finns Ledningssystem för informationssäkerhet med krav och råd om säkerhet i svensk standard för informationssäkerhet, SS-ISO/IEC 27002, som ingår i ISO 27000-serien och ger en heltäckande bild över hur information bör hanteras.

Krisberedskapsmyndigheten (numera Myndigheten för samhällsskydd och beredskap) har också framarbetat produkten Basnivå för informationssäkerhet, BITS.

## **5.2 Grundläggande principer för skydd av information vid överföring och lagring**

Grundläggande principer för att skydda uppgifter och följa upp inträffade händelser i informationssystem är autentisering (kontroll av uppgiven identitet), auktorisation (styrning av åtkomsträttigheter), konfidentialitet (sekretess), riktighet (dataintegritet), tillgänglighet, och spårbarhet (loggning).

Med informationssäkerhet menas förmågan att upprätthålla dessa principer avseende informationstillgångar. Åtgärder bör vidtas för att *rätt person* ska få tillgång till *rätt data* i *rätt tid*. Dessutom bör åtgärder vidtas för att förebygga att tillgångar skadas eller förstörs. Skyddsåtgärderna bör även göra det möjligt att upptäcka när, hur och av vem en tillgång har skadats, och tillåta att man kan återfå sina tillgångar eller reparera inträffade skador. Nedan beskrivs de grundläggande principerna närmare.

#### Autentisering

Autentisering innebär kontroll av uppgiven identitet och är en viktig funktion i IT- och informationssystem. Autentisering kan t.ex. genomföras med hjälp av något användaren vet, har eller är. Genom att användaren anger ett användarnamn och t.ex. ett lösenord (något användaren vet) kan autentiseringen ske av denne.

Vid överföring av uppgifter i syfte att användas i mobila innehållstjänster, tillämpar mobiloperatörerna ett autentiseringsförfarande innan aggregatörer och innehållsleverantörer får tillgång till operatörernas plattformar. Vid autentiseringen uppger innehållsleverantören eller aggregatören vanligen ett användarnamn och lösenord, som denne har fått tilldelat av operatören för åtkomst till systemet. Autentisering av aktörer sker även genom att tillgång till operatörens plattform endast medges från vissa IP-adresser och vissa portnummer.

Tack vare ett autentiseringsförfarande kan operatören få vetskap om vilka aktörer som har åtkomst till systemet. Autentisering kan även möjliggöra spårbarhet och användas för att följa upp inträffade händelser/transaktioner i systemet.

#### Auktorisation

Auktorisation innebär tilldelning av åtkomsträttigheter och kontroll av behörighet i ett s.k. behörighetskontrollsystem. Åtkomsträttigheter kan sättas för t.ex. en användare, ett program, en process, ett filsystem etc. Behörighet och behörighetskontroll kan realiseras genom en s.k. åtkomsträttighetslista/behörighetslista (Access Control List, ACL). En sådan lista specificerar vem som ges åtkomst till vad, liksom vilka åtgärder (läsa, skriva, kopiera) som tillåts. Behörighetsprofilen bör endast medge den åtkomst som krävs för att det avtalade ändamålet ska uppfyllas.

Av uppgifterna från mobiloperatörerna framgår att det är vanligt med behörighetskontrollsystem i systemen som tillhandahåller uppgifter för mobila innehållstjänster.

#### Riktighet

Vid informationsutbyte och lagring är det viktigt att kunna säkerställa att information inte har ändrats. Riktighet innebär att information inte av misstag eller obehörigen har förändrats och i fallet med mobila innehållstjänster innebär det t.ex. att beställt innehåll, debiteringsinformation och abonnentens telefonnummer inte förändras under överföringen eller lagringen av dessa uppgifter. Riktighet av information kan tillförsäkras genom användning av t.ex. checksummor och kryptering.

#### Konfidentialitet

Konfidentialitet innebär skydd av information från obehörig insyn. Det sker ofta genom kryptering av information i system eller av själva överföringen av information. Kryptering medför att information inte skickas i klartext, och skyddar inte enbart mot obehörig insyn utan kan, som påpekats ovan, också användas för att upprätthålla riktigheten i informationen.

#### Spårbarhet

Spårbarhet är en viktig säkerhetsåtgärd för att kunna upptäcka obehörig informationsbehandling. Med spårbarhet menas att användaridentitet, datum och tidpunkt för t.ex. in- och utloggning eller lyckade och misslyckade försök till åtkomst, registreras. Det är vidare lämpligt att policier finns för hur ofta loggarna ska analyseras, vem som ansvarar för analys av dem, hur länge de ska sparas och hur de ska förvaras (för att skyddas mot t.ex. otillbörlig åtkomst).

### **5.3 Kommunikationen mellan aktörerna och de tekniker som används**

I det här kapitlet beskrivs översiktligt, med utgångspunkt i aktörernas redogörelser, hur kommunikationen mellan mobilanvändaren och innehållsleverantören, via operatör och eventuell aggregatör, går till och vilka överföringstekniker som används. En kort förklaring av de tekniska begrepp som används återfinns i bilaga 4.

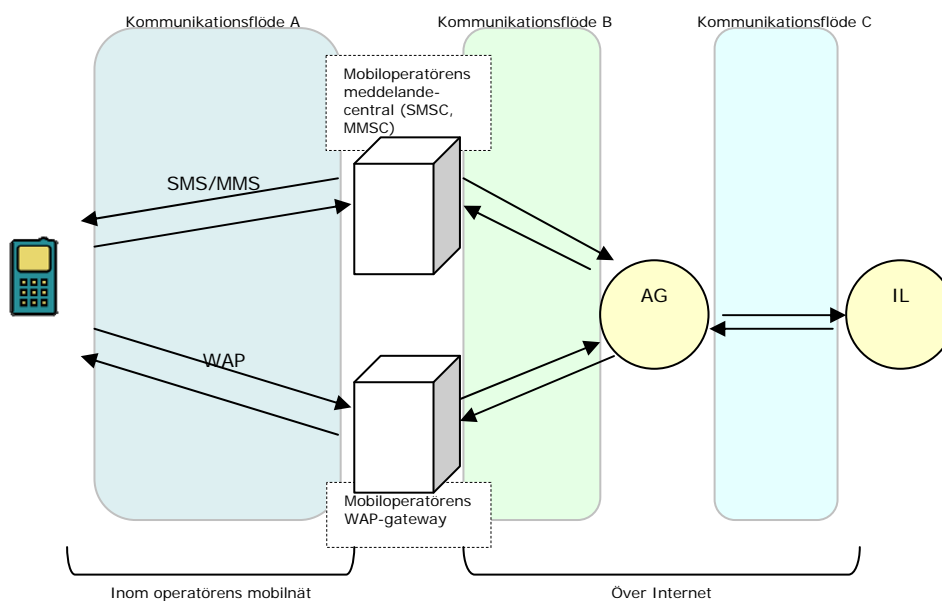
Kommunikationen mellan mobilanvändare och innehållsleverantör för förmedling av innehåll

Idag kan många mobiltelefoner använda flera olika slags tekniker för kommunikation. Som har beskrivits i kapitel 3 förekommer beställning av innehåll och tjänster, liksom leverans av det beställda innehållet, via såväl sms- och mms-meddelanden som WAP- eller webböverföring. I den här rapporten beaktas endast de fall där mobiltelefonen kommunicerar över ett mobilnät, dvs. över ett GSM- eller UMTS-baserat nät.

När en mobilanvändare beställer en mobil innehållstjänst via sms eller mms skickas beställningen via operatörens nät till en s.k. meddelandecentral (SMSC respektive MMSC) (se figur 2, kommunikationsflöde A). Från meddelandecentralen skickas meddelandet som innehåller beställningen tillsammans med slutkundens telefonnummer över Internet till innehållsleverantören eller aggregatören (kommunikationsflöde B och C). Oftast skickas informationen mellan operatör och innehållsleverantör respektive aggregatör med hjälp av http, men i vissa fall används en krypterad förbindelse i form av https eller VPN-teknik.

I det fall användaren kontaktar en mobil innehållstjänst genom sin mobiltelefons WAP-läsare överförs informationen via mobiloperatörens WAP-gateway (kommunikationsflöde A), där de överförda meddelandena förses abonnentens telefonnummer i den s.k. WAP-headern. Denna information kan sedan utläsas av innehållsleverantören och användas för att hålla ordning på vem som besökt dennes WAP-tjänst och genomfört eventuella beställningar.

Figur 2. Kommunikationsflöden över olika tekniker som används för att förmedla en innehållstjänst



Kommunikationen mellan innehållsleverantör och operatör för debitering och positionering

En innehållsleverantör, alternativt en aggregatör, och en operatör kan även ingå avtal om att innehållsleverantören eller aggregatören ska få tillgång till operatörens system, för debitering av abonnenter eller för positionering av mobiltelefoner. Det varierar hur överföringen i dessa fall går till. I vissa fall används även här http-baserad överföring, medan trafiken i andra fall överförs med hjälp av VPN.

#### **5.4 Tekniska åtgärder för att skydda uppgifter vid överföring och vid lagring**

I det här avsnittet beskrivs kortfattat de tekniska åtgärder som vidtagits för att skydda de uppgifter som överförs mellan aktörerna. Inledningsvis redogörs för några av de skyddsmekanismer som är inbyggda i de överföringstekniker som används. Därefter beskrivs vilka åtgärder aktörerna själva har vidtagit för att skydda informationen.

Skyddsmekanismer som finns inbyggda i de överföringstekniker som används I mobiltekniken GSM finns ett antal specificerade säkerhetsfunktioner. GSM använder sig bl.a. av olika kryptoalgoritmer för att upprätthålla konfidentialiteten vid överföringen. Det bör dock påpekas att denna kryptering endast används över radiogränssnittet, dvs. mellan basstationen och mobiltelefonen.

Säkerhetsfunktionerna i UMTS bygger på de i GSM-tekniken, men i UMTS har dessa förbättrats. För att uppnå konfidentialitet använder man sig av starkare kryptoalgoritmer och längre kryptonycklar än i GSM. Dessutom krypteras inte enbart trafiken över radiogränssnittet utan även en del av trafiken i den trådbundna infrastrukturen (trafiken från basstationen till den första noden).

GPRS-tekniken, som används för att överföra data i GSM-nät, har inga egna funktioner för att uppnå konfidentialitet. Överföring via GPRS skyddas dock av de säkerhetsfunktioner som finns i GSM-tekniken.

Information som skickas med http, skickas normalt i klartext men genom att istället använda https förses överföringen med kryptering.

Åtgärder som har vidtagits av aktörerna

Mobiloperatörerna har uppgett att en krypterad förbindelse, i form av https eller VPN, i vissa fall används för överföring av uppgifter *mellan operatörer och innehållsleverantörer respektive aggregatörer*. VPN-teknik används dock nästan uteslutande vid överföring av uppgifter i samband med positionering.

Flertalet operatörer och aggregatörer anger att de använder autentisering och auktorisation genom användning av accesslistor över innehållsleverantörernas respektive aggregatörernas IP-adresser, så att bara dessa IP-adresser kan ansluta mot operatörens system. De flesta operatörer loggar också händelser i sina system, i syfte att kunna upptäcka fel eller intrång.

Några av operatörerna har även uppställt säkerhetskrav i avtal gentemot innehållsleverantörer och aggregatörer. Enligt avtalen ansvarar innehållsleverantörer/aggregatörer för att tillhandahålla tekniska och organisatoriska säkerhetsåtgärder som är nödvändiga för att skydda uppgifterna från oavsiktlig eller förstörelse, förlust samt oauktoriserad förmedling av eller tillgång uppgifter.

Av aggregatörernas och innehållsleverantörernas uppgifter framgår att kommunikation som sker mellan aggregatörer och innehållsleverantörer skyddas i varierande grad. När det gäller överföring av lokaliseringssuppgifter är kommunikationen krypterad. När det gäller exempelvis telefonnummer skickas det i vissa fall i klartext och i andra fall krypterat. Någon enstaka aggregatör använder VPN-förbindelser för kommunikationen med innehållsleverantörer.

Som framgått ovan är innehållsleverantören vanligen personuppgiftsansvarig för behandlingen hos denne och hos aggregatören och därmed även ansvarig för säkerheten. PTS och Datainspektionen kan dock konstatera att kommunikationen med operatörer i praktiken styrs av de säkerhetslösningar som används av och de krav som ställs, av operatörerna.

## 6 Slutsatser och rekommendationer

### Sammanfattning

---

Efter den genomförda tillsynen vill myndigheterna lyfta fram några slutsatser som särskilt viktiga och baserat på dessa lämna rekommendationer.

En sådan rekommendation är att operatörer bör undvika att utforma system för t.ex. positionering och debitering så att telefonnummer används för identifiering av abonnenten. Myndigheterna anser att det borde vara tillräckligt att använda en mer anonym uppgift, som endast operatören kan härleda till den aktuella abonnenten.

En generell rekommendation är att integritetsfrågor bör beaktas redan när tjänster tas fram. Det kan ofta vara både svårare och dyrare att förbättra integritetsskyddet i efterhand.

Myndigheterna rekommenderar aktörerna att se över sina rutiner för samtycke och information, i ljuset av de slutsatser som myndigheterna dragit om fördelningen av ansvaret för hantering av trafikuppgifter.

Slutligen rekommenderas aktörerna att generellt beakta säkerhetsfrågor vid utformningen av tjänster. Det är bl.a. lämpligt att arbeta med informationsklassning och riskanalyser. Det kan ofta också vara lämpligt att skydda uppgifter genom säkra autentiseringsförfaranden och genom att använda kryptering. Autentisering och transaktioner bör också loggas för att åstadkomma spårbarhet.

I detta kapitel redogörs kortfattat för några av de viktigare slutsatser som myndigheterna har dragit av den tillsyn som genomförts mot operatörer, aggregatörer och innehållsleverantörer. Avsikten är inte att peka på brister hos enskilda aktörer utan att lämna generella rekommendationer som bör beaktas av branschen som helhet. Myndigheterna anser att aktörerna i huvudsak har en tillfredsställande hantering av de uppgifter som överförs, men vill dock göra vissa påpekanden. Det finns därmed utrymme för förbättring och utveckling.

## **6.1 Rekommendationer för ökad hänsyn till integritet**

### **6.1.1 Telefonnummer bör undvikas för identifiering**

Myndigheterna anser att aktörerna så långt som möjligt bör utgå från metoder som tillvaratar användarnas integritetsskydd i sin verksamhet och att just telefonnummer som identifieringsuppgift därför inte bör överföras i de fall det inte behövs.

Av de uppgifter som aktörer har lämnat framgår att uppgift om abonnentens telefonnummer i flertalet fall utbyts mellan operatörer och innehållsleverantörer, i syfte att kunna identifiera och fakturera abonnenten (se figur 1 i kapitel 3.2 ovan). I de fall användaren kommunicerar med innehållsleverantören via sms eller mms torde det som regel vara så att användaren förstår att telefonnumret kan förmedlas i transaktionen (detta är ju normalfallet för sådana meddelanden) och att det därför också kan användas för fakturering av tjänsten.

När det gäller tillhandahållande av innehållstjänster via webben är förhållandet inte alls lika självklart och man kan snarast utgå från att abonnenten inte inser att dennes telefonnummer överförs till webbplatsinnehavaren, när mobiltelefonen används för att besöka en webbplats.

Situationen blir också mer problematisk när det gäller överföring av telefonnummer till webbplatser som tillhandahåller såväl innehållstjänster mot betalning som kostnadsfritt innehåll, t.ex. information och nyheter. I dessa fall åtföljer, såvitt myndigheterna kan förstå av de uppgifter operatörerna lämnat, i många fall abonnentens telefonnummer med webbsessionen, oavsett om användaren söker åtkomst till en innehållstjänst eller det kostnadsfria innehållet. Innehavaren av webbplatsen får således kunskap om besökarens telefonnummer även i de fall detta inte är nödvändigt för debitering av en innehållstjänst.

Situationen kan förvisso jämföras med att webbplatsinnehavare får uppgift om de IP-adresser som tillhör de som besöker webbplatsen. Detta är dock en teknisk förutsättning för att kommunikationen ska fungera och sådana uppgifter överförs utan att webbplatsinnehavaren har ingått ett särskilt avtal med operatören om att få åtkomst till dessa. I likhet med ett telefonnummer utgör IP-adressen en trafikuppgift och i många fall även en personuppgift. En IP-adress kan dock ur integritetssynpunkt inte enkelt jämföras med ett telefonnummer eftersom IP-adressen normalt inte på något enkelt sätt kan härledas till en fysisk individ. Det är endast den operatör som abonnenten använder för sin Internetanslutning som har tillgång till information om vilken IP-adress som tilldelats en viss person vid en viss tidpunkt. Ett telefonnummer

kan däremot i de flesta fall enkelt härledas till en viss abonnent av vem som helst, inte bara operatören.

Överföring av telefonnummer i webbsessioner utgör inte någon teknisk förutsättning för att kommunikationen ska fungera, utan är uppgifter som lagts till för att möjliggöra en identifikation av besökaren. Abonnenter kan i vissa fall uppleva det som integritetskränkande att det så pass enkelt går att avgöra vem som vid ett visst tillfälle besökte en viss webbplats och även vilka individuella webbsidor personen tagit del av.

Från en tekniskt effektiv synvinkel är det förståeligt att man inom branschen använder sig av telefonnummer, eftersom de är unika för varje abonnent samt följer ett standardiserat format som är detsamma oavsett operatör. Därmed kan de lätt användas för identifiering av abonnenten och i ett eventuellt nästa steg fakturering av densamme. De lösningar som är tekniskt enklast är dock inte alltid utifrån en integritetsrättslig synpunkt de lämpligaste. För att identifiera användaren borde det vara tillräckligt att använda en mer anonym uppgift, som endast operatören kan härleda till den aktuella abonnenten. En av operatörerna uppger också att man utbyter ett unikt kundnummer med innehållsleverantören.

Det bör påpekas att det ur en strikt juridisk synvinkel inte har någon betydelse om endast ett fåtal kan härleda en uppgift till en viss person eller inte; så länge en uppgift kan utpeka en levande person anses det utgöra en personuppgift varför behandlingen av sådana uppgifter är underställt de krav som finns i PuL. Detta gäller således såväl telefonnummer som IP-adresser och ev. kundnummer.

#### **6.1.2 Integritet bör beaktas redan när tjänster tas fram**

Myndigheterna har förståelse för att aktörerna försöker finna effektiva lösningar, men anser att aktörerna i högre utsträckning bör låta integritetsaspekter genomsyra utformandet av tjänsterna redan vid deras framtagande.

Som fallet med överföringen av telefonnummer i identifieringssyfte visar, är det viktigt att aktörer på marknaden uppmärksammar inte bara kravet utan också behovet av att ta hänsyn till integritetsrelaterade frågeställningar redan när tjänster utvecklas. Att integritetsfrågor beaktas som en självklar del av processen när tjänster utvecklas, är inte bara åtråvärt ur ett myndighetsperspektiv utan sannolikt också utifrån ett kundrelationsperspektiv och inte minst ett ekonomiskt perspektiv. Det kan vara komplicerat och dyrt

att förändra en tjänst som redan är framtagen, om det skulle komma att krävas, t.ex. för att efterkomma krav från myndigheter.

Myndigheternas reflektion vid bedömningen av de tjänster som berörs i denna rapport är att hänsyn verkar ha tagits till integritetsaspekter när hanteringen av lokaliseringssuppgifter har utformats. Detta har lett till att skydd för integriteten generellt tycks ha byggts in i större utsträckning i positioneringstjänster. Som jämförelse med detta är myndigheternas åsikt att samma hänsyn till integritetsaspekter inte alls tagits angående användning av telefonnummer i identifikationssyfte för mobila innehållstjänster via webben.

### **6.1.3 Aktörerna bör se över rutiner för samtycke och information**

Det är varje aktörs ansvar att se till att denne har en rättslig grund för sin behandling. Det är myndigheternas uppfattning att det är lämpligt ur ett integritetsperspektiv att innehållsleverantörerna, även i de fall detta inte är ett lagstadgat krav, använder sig av samtycke som grund för behandling av uppgifter vid tillhandahållande av mobila innehållstjänster. För operatörernas behandling är samtycke alltid ett krav. Den som stödjer sin behandling på samtycke från användaren måste se till att användaren får tillräcklig information om den tilltänkta behandlingen i samband med att samtycket inhämtas. Annars är samtycket inte giltigt.

Det är alltid viktigt att vara noga med informationen till användarna – oavsett om grunden för behandlingen är samtycke eller inte. Informationen bör lämnas på det sätt som är lämpligast för den aktuella innehållstjänsten. Den kan lämnas vid användning av tjänsten eller i t.ex. avtalsvillkor. Innehållsleverantörer måste vara noga med att tydligt ange identitet och kontaktuppgifter till den som är personuppgiftsansvarig. De måste också se till att lämna information om den registrerades rätt till registerutdrag och möjligheten att begära rättelse.

Ovan har redogjorts för myndigheternas bedömningar när det gäller gränsdragningen mellan LEK och PuL liksom närmare bedömningar när det gäller hur och när samtycke måste inhämtas, och av vem. Av svaren på tillsynsenkäterna framgår att aktörernas egna bedömningar i dessa frågor skiljer sig åt. Operatörerna har inte i detalj beskrivit de bedömningar som ligger till grund för de rutiner som idag tillämpas, varför det inte är möjligt att uttala sig om bedömningarna i det enskilda fallet varit riktiga. Att bedömningarna tycks skilja sig åt tyder dock på att det kan finnas anledning för aktörerna att se över sina rutiner, i ljuset av de bedömningar som myndigheterna gjort i denna rapport.

## **6.2 Rekommendationer för ökad säkerhet vid överföring av uppgifter**

### **6.2.1 Informationsklassning och riskanalyser bör genomföras**

Det kan inledningsvis konstateras att en lämplig grund för allt informationssäkerhetsarbete kan uppnås genom att identifiera vilka informationstillgångar som finns i organisationen och klassificera dessa avseende konfidentialitet, riktighet och tillgänglighet, med hänsyn tagen till organisationens krav på skyddsnivå. Detta arbete bör genomföras med hjälp av riskanalyser, där hot riktade mot exempelvis organisationens informationstillgångar identifieras och en bedömning görs av sannolikheten för att hotet inträffar och vilka konsekvenser detta kan få.

### **6.2.2 Åtkomsträttigheter bör begränsas och autentisering användas**

Det är viktigt att definiera vilka informationstillgångar och system respektive användare<sup>7</sup> ska ha tillgång till samt vilka funktioner användaren får utföra. Åtkomsträttigheterna bör begränsas till vad som är nödvändigt för att användaren, ska kunna utföra de åtgärder som denne har ett berättigat behov av och befogenhet att utföra.

För att kunna tillämpa behörigheterna krävs att användare autentiseras med hjälp av ett system för verifikation av uppgiven identitet. Av de uppgifter som lämnats till myndigheterna framgår att operatörer redan idag autentiserar innehållsleverantörer och aggregatörer, men att olika metoder används.

### **6.2.3 Kryptering bör användas när trafikuppgifter överförs**

När abonnenters telefonnummer eller lokaliseringssuppgifter skickas över ett öppet nät, som Internet, är det lämpligt att skydda uppgifterna från avlyssning genom att använda kryptering. Kryptering medför också att informationen inte kan förvanskas av obehöriga, under överföringen.

När till exempel kommunikationen mellan mobilanvändare och innehållsleverantörer sker över WAP, skickas uppgift om användarens telefonnummer i klartext, i http-headern. Detta kan i viss utsträckning undvikas genom att istället använda https för överföringen. Vad gäller överföringen av telefonnummer på detta sätt, se även kapitel 6.1.1.

### **6.2.4 Autentisering och transaktioner bör loggas**

För att kunna gå tillbaka och spåra vilka som haft åtkomst till ett visst system, när så skedde och vilka uppgifter som behandlades, krävs att sådan information

---

<sup>7</sup> I relation till mobila innehållstjänster avses här en innehållsleverantör eller en aggregatör som ges tillgång till en annan aktörs system.

kontinuerligt loggas i systemet. Det är myndigheternas uppfattning att sådan loggning bör användas där så är möjligt.

Av de uppgifter som lämnats av operatörerna framgår att de flesta loggar händelser i de system som tillhandahåller uppgifter för mobila innehållstjänster, dock inte alla. Någon uppger att det i första hand ligger på innehållsleverantören att utföra sådan loggning. Detta är dock normalt inte tillräckligt, eftersom t.ex. obehörig åtkomst till operatörens system inte kan upptäckas i de loggar som förs av innehållsleverantörer.

## 7 Myndigheternas fortsatta arbete

### Sammanfattning

---

PTS har även för avsikt att fortsätta följa utvecklingen inom området för mobila innehållstjänster och tjänster som bygger på positionering. Myndigheten vill arbeta för att bidra till att integritetsfrågorna beaktas i operatörernas behandling.

Datainspektionen kommer fortsättningsvis att granska innehållsleverantörers och aggregatörers personuppgiftsbehandling inom ramen för den ordinära tillsynsverksamheten.

Under inledningen av 2010 kommer slutsatserna i rapporten att presenteras på Integritetsforum.

### 7.1 PTS fortsatta arbete

Den tillsynsaktivitet som inleddes den 9 juni 2009 och riktades mot fyra operatörer, har i och med denna rapport avslutats. Vad som framkommit har inte gett myndigheten anledning att vidta några ytterligare omedelbara tillsynsåtgärder. Operatörernas hantering av de integritetsfrågor som berörts ovan kommer dock att följas upp.

PTS har även för avsikt att fortsätta följa utvecklingen inom området i stort och genom såväl tillsynsinsatser som andra aktiviteter söka bidra till att integritetsfrågorna beaktas i operatörernas behandling av de uppgifter som regleras i LEK, liksom i utformningen av tjänster där sådana uppgifter förekommer.

Detta gäller särskilt tjänster som bygger på positionering. Sådana tjänster kommer sannolikt att utvecklas i snabb takt och i större utsträckning nyttja flera alternativa tekniker, såsom t.ex. GPS och Bluetooth. Det kan därför finnas anledning för PTS att framöver ta ställning till hur den integritetsrelaterade regleringen i LEK ska tillämpas i förhållande till användningen av sådana tekniker.

PTS har för avsikt att under inledningen av 2010 presentera slutsatserna i denna rapport på Integritetsforum; de möten för information och diskussion om aktuella integritetsfrågor som regelbundet anordnas av PTS.

Avslutningsvis kan nämnas att myndigheten också bedriver arbete med andra frågor som rör mobila innehållstjänster. Det gäller framförallt konsumentfrågor, såsom hur tjänsterna marknadsförs, vilken information som lämnas till konsumenter i samband med beställning och de avtalsvillkor som tillämpas av innehållsleverantörerna. I sammanhanget kan nämnas att PTS, i en undersökning under våren 2009 om konsumenters förhållande till Internetsäkerhet, bad de tillfrågade beskriva sin inställning till positioneringstjänster.<sup>8</sup> Denna undersökning kommer följas upp regelbundet för att undersöka utvecklingen av konsumenters förhållande till dessa företeelser.

## **7.2 Datainspektionens fortsatta arbete**

Datainspektionen har för närvarande inga planer på att följa upp projektet. Innehållsleverantörers och aggregatörers personuppgiftsbehandling kommer dock, i den mån det blir aktuellt, att granskas inom ramen för den ordinära tillsynsverksamheten.

---

<sup>8</sup> Se PTS rapport "Konsumenters förhållande till Internetsäkerhet - En undersökning om kunskap, beteende och tillit", PTS-ER-2009:18. Rapporten finns i sin helhet på <http://www.pts.se/upload/Rapporter/Internet/2009/2009-18-konsumenternas-forhallande-till-internetsakerhet.pdf>.

## Litteratur

### Författningar och förarbeten

*Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.*

*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).*

*Lag (2003:389) om elektronisk kommunikation.*

*Lag om elektronisk kommunikation m.m., proposition 2002/03:110.*

*Personuppgiftslagen (1998:204).*

### Föreskrifter och allmänna råd

*Datainspektionen, 2008, Allmänna råd - Säkerhet för personuppgifter.*  
<http://www.datainspektionen.se/Documents/faktabroschyr-allmannarad-sakerhet.pdf>.

### Rapporter m.m.

*Krisberedskapsmyndigheten, 2006, Basnivå för informationssäkerhet (BITS) (KBM Rekommenderar 2006:1).*  
[http://www2.msb.se/upload/Publikationsservice/KBM/rekommenderar/bits\\_rek\\_2006\\_1.pdf](http://www2.msb.se/upload/Publikationsservice/KBM/rekommenderar/bits_rek_2006_1.pdf).

*Post- och telestyrelsen, 2009, Konsumenters förhållande till Internetsäkerhet - En undersökning om kunskap, beteende och tillit (PTS-ER-2009:18).*  
<http://www.pts.se/upload/Rapporter/Internet/2009/2009-18-konsumenternas-forhallande-till-internetsakerhet.pdf>.

*Post- och telestyrelsen, 2006, Sammanställning av lagstiftning och praxis kring utlämnande av teleuppgifter.*  
[http://www.pts.se/upload/Documents/SE/sammanstallning\\_lagstiftning\\_teleuppgifter%202006-11-28.pdf](http://www.pts.se/upload/Documents/SE/sammanstallning_lagstiftning_teleuppgifter%202006-11-28.pdf).

### Övriga källor

*SIS – Ledningssystem, 2008, Ledningssystem för informationssäkerhet (SS-ISO/IEC 27002:2005).*

## Bilaga 1 – Definitioner och förklaring av grundläggande begrepp

Här följer en förklaring av några grundläggande begrepp som används i rapporten. I de fall ett begrepp har definierats i lag och det används med samma innebörd i rapporten, anges här den lagstadgade definitionen (med lagrum angivet inom parentes). I övriga fall beskrivs hur begreppet används i denna rapport.

**Abonnent** – Den som har ingått avtal med en leverantör av allmänt tillgängliga elektroniska kommunikationstjänster om tillhandahållande av sådana tjänster. (1 kap. 7 § LEK).

**Abonnentuppgifter** – Uppgifter som relativt statistiskt är kopplade till abonnenten såsom abonnentens namn, adress och telefonnummer (kan även benämnas uppgift om abonnemang).

**Aggregatör** – Den som agerar mellanhand mellan innehållsleverantörer och operatörer. Aggregatören tillhandahåller ett tekniskt system som förenklar överföring av uppgifter mellan innehållsleverantörer och samtliga operatörer.

**Användare** – Den som använder eller efterfrågar en allmänt tillgänglig elektronisk kommunikationstjänst. (1 kap. 7 § LEK).

**Behandling av personuppgifter** – Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning, eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring. (3 § PuL).

**Den registrerade** – Den som en personuppgift avser. (3 § PuL).

**Elektronisk kommunikationstjänst** – Tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät. (1 kap. 7 § LEK).

**Elektroniskt meddelande** – All information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst [...]. (6 kap. 1 § LEK).

**Identifikationssyfte** – När uppgifter överförs i samband med tillhandahållandet av en innehållstjänst, för att möjliggöra identifikation av en abonnent och för fakturering av densamme.

**Innehållsleverantör** – Den som tillhandahåller innehåll över en elektronisk kommunikationstjänst.

**Lokaliseringsuppgifter** – Uppgift som behandlas i ett kommunikationsnät och som anger den geografiska positionen för en användares terminalutrustning. (1 kap. 7 § LEK).

**Lokaliseringssyfte** – När uppgifter överförs för att möjliggöra lokalisering av användaren i en innehållstjänst.

**Operatör** – I denna rapport avses med begreppet endast tillhandahållare av elektronisk kommunikationstjänst för mobiltelefoni.

**Personuppgifter** – All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. (3 § PuL).

**Personuppgiftsansvarig** – Den som ensam eller tillsammans med andra bestämmer ändamålen, dvs. syftet med och medlen för behandlingen av personuppgifter. (3 § PuL).

**Personuppgiftsbiträde** – Den som behandlar personuppgifter för den personuppgiftsansvariges räkning. (3 § PuL).

**Samtycke** – Varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne. (3 § PuL).

**Trafikuppgifter** – Uppgifter som behandlas i syfte att befordra elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande (6 kap. 1 § LEK).

**Uppdragstjänst** – En innehållstjänst som levereras på uppdrag av en operatör, i enlighet med bestämmelserna i 6 kap. 7 § LEK.

## Bilaga 2 – Utdrag ur relevant lagstiftning

### 1. Lagen (2003:389) om elektronisk kommunikation

6 kapitlet

5 § Trafikuppgifter som avser användare som är fysiska personer eller avser abonnenter och som lagras eller behandlas på annat sätt av den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 §, ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande, om de inte får sparas för sådan behandling som anges i 6 eller 13 §.

6 § Trafikuppgifter som krävs för abonnentfakturerings och betalning av avgifter för samtrafik får behandlas till dess att fordran är betald eller preskription inträtt och det inte längre lagligen går att göra invändningar mot faktureringen eller avgiften.

Om den som uppgifterna rör har samtyckt till det, får den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst behandla de uppgifter som avses i 5 § för att marknadsföra elektroniska kommunikationstjänster eller för att tillhandahålla andra tjänster där uppgifterna behövs, i den utsträckning och under den tid som är nödvändig för tjänsten eller marknadsföringen. Ett samtycke kan när som helst återkallas.

Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska informera den uppgiften rör om vilken typ av trafikuppgifter som behandlas och hur länge uppgifterna behandlas för sådana ändamål som anges i första och andra stycket. Informationen ska lämnas innan samtycke inhämtas.

7 § Behandling av trafikuppgifter enligt 5 och 6 §§ får utföras endast av den som fått i uppdrag av den som bedriver verksamhet som är anmälningspliktig att sköta fakturering, trafikstyrning, kundförfrågningar, marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av andra tjänster där uppgifterna behövs. Behandlingen ska begränsas till vad som är nödvändigt för verksamheten.

17 § Utöver vad som anges i 5-7 och 20 §§ får inte någon annan än berörda användare ta del av eller på annat sätt behandla uppgifter i ett elektroniskt

meddelande som överförs i ett allmänt kommunikationsnät eller med en allmänt tillgänglig elektronisk kommunikationstjänst, eller trafikuppgifter som hör till detta meddelande, om inte en av användarna har samtyckt till behandlingen. [...]

## 2. Personuppgiftslagen (1998:204)

### *Allmänna bestämmelser*

#### *Avvikande bestämmelser i annan författning*

2 § Om det i en annan lag eller i en förordning finns bestämmelser som avviker från denna lag, skall de bestämmelserna gälla.

#### *Det territoriella tillämpningsområdet*

4 § Denna lag gäller för sådana personuppgiftsansvariga som är etablerade i Sverige.

Lagen tillämpas också när den personuppgiftsansvarige är etablerad i tredje land men för behandlingen av personuppgifter använder sig av utrustning som finns i Sverige. Vad som nu sagts gäller dock inte om utrustningen bara används för att överföra uppgifter mellan ett tredje land och ett annat sådant land.

I det fall som avses i andra stycket första meningen skall den personuppgiftsansvarige utse en företrädare för sig som är etablerad i Sverige. Vad som anges i denna lag om den personuppgiftsansvarige skall också gälla för företrädaren.

#### *Behandling av personuppgifter som omfattas av lagen*

5 § Denna lag gäller för sådan behandling av personuppgifter som helt eller delvis är automatiserad.

Lagen gäller även för annan behandling av personuppgifter, om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

#### *Undantag för behandling av personuppgifter i ostrukturerat material.*

**5 a §** Bestämmelserna i 9, 10, 13-19, 21-26, 28, 33, 34 och 42 §§ behöver inte tillämpas på behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter.

Sådan behandling som avses i första stycket får inte utföras, om den innebär en kränkning av den registrerades personliga integritet. Lag (2006:398).

*Grundläggande krav på behandlingen av personuppgifter*

**9 §** Den personuppgiftsansvarige skall se till att

- a) personuppgifter behandlas bara om det är lagligt,
- b) personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed,
- c) personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål,
- d) personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in,
- e) de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,
- f) inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,
- g) de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella,
- h) alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen, och
- i) personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

I fråga om första stycket d gäller dock att en behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte skall anses som oförenlig med de ändamål för vilka uppgifterna samlades in.

Personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål under längre tid än som sagts i första stycket i. Personuppgifterna får dock i sådana fall inte bevaras under en längre tid än vad som behövs för dessa ändamål.

Personuppgifter som behandlas för historiska, statistiska eller vetenskapliga ändamål får användas för att vidta åtgärder i fråga om den registrerade bara om

den registrerade har lämnat sitt samtycke eller det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

*När behandling av personuppgifter är tillåten*

**10 §** Personuppgifter får behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen eller om behandlingen är nödvändig för att

- a) ett avtal med den registrerade skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas,
- b) den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet,
- c) vitala intressen för den registrerade skall kunna skyddas,
- d) en arbetsuppgift av allmänt intresse skall kunna utföras,
- e) den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller
- f) ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut skall kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.

*Förbud mot behandling av känsliga personuppgifter*

**13 §** Det är förbjudet att behandla personuppgifter som avslöjar

- a) ras eller etniskt ursprung,
- b) politiska åsikter,
- c) religiös eller filosofisk övertygelse, eller
- d) medlemskap i fackförening.

Det är också förbjudet att behandla sådana personuppgifter som rör hälsa eller sexualliv.

Uppgifter av den art som anges i första och andra styckena betecknas i denna lag som känsliga personuppgifter.

***Information till den registrerade***

*Information skall lämnas självmant*

**23 §** Om uppgifter om en person samlas in från personen själv, skall den personuppgiftsansvarige i samband därmed självmant lämna den registrerade information om behandlingen av uppgifterna.

**24 §** Om personuppgifterna har samlats in från någon annan källa än den registrerade, skall den personuppgiftsansvarige självant lämna den registrerade information om behandlingen av uppgifterna när de registreras. Är uppgifterna avsedda att lämnas ut till tredje man, behöver informationen dock inte ges förrän uppgifterna lämnas ut för första gången.

Information enligt första stycket behöver inte lämnas, om det finns bestämmelser om registrerandet eller utlämnandet av personuppgifterna i en lag eller någon annan författning.

Information behöver inte heller lämnas enligt första stycket, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Om uppgifterna används för att vidta åtgärder som rör den registrerade, skall dock information lämnas senast i samband med att så sker.

*Den information som skall lämnas självant*

**25 §** Information enligt 23 eller 24 § skall omfatta

- uppgift om den personuppgiftsansvariges identitet,
- uppgift om ändamålen med behandlingen, och
- all övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse.

Information behöver dock inte lämnas om sådant som den registrerade redan känner till.

*Information skall lämnas efter ansökan*

**26 §** Den personuppgiftsansvarige är skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som rör den sökande behandlas eller ej. Behandlas sådana uppgifter skall skriftlig information lämnas också om

- vilka uppgifter om den sökande som behandlas,
- varifrån dessa uppgifter har hämtats,
- ändamålen med behandlingen, och
- till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

En ansökan enligt första stycket skall göras skriftligen hos den personuppgiftsansvarige och vara undertecknad av den sökande själv. Information enligt första stycket skall lämnas inom en månad från det att

ansökan gjordes. Om det finns särskilda skäl för det, får information dock lämnas senast fyra månader efter det att ansökan gjordes.

Information enligt första stycket behöver inte lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Vad som nu sagts gäller dock inte om uppgifterna har lämnats ut till tredje man eller om uppgifterna behandlas enbart för historiska, statistiska eller vetenskapliga ändamål eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

#### *Rättelse*

**28 §** Den personuppgiftsansvarige är skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har utfärdats med stöd av lagen. Den personuppgiftsansvarige skall också underrätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

#### ***Säkerheten vid behandling***

##### *Personer som behandlar personuppgifter*

**30 §** Ett personuppgiftsbiträde och den eller de personer som arbetar under bitrådets eller den personuppgiftsansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige.

Det skall finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet skall det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 31 § första stycket.

Om det i lag eller annan författning finns särskilda bestämmelser om behandlingen av personuppgifter i det allmännas verksamhet i frågor som avses i första stycket, skall dessa gälla i stället för vad som sägs i första stycket.

### *Säkerhetsåtgärder*

**31 §** Den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av

- a) de tekniska möjligheter som finns,
- b) vad det skulle kosta att genomföra åtgärderna,
- c) de särskilda risker som finns med behandlingen av personuppgifterna, och
- d) hur pass känsliga de behandlade personuppgifterna är.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, skall den personuppgiftsansvarige förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

### ***Överföring av personuppgifter till tredje land***

#### *Förbud mot överföring av personuppgifter till tredje land*

**33 §** Det är förbjudet att till tredje land föra över personuppgifter som är under behandling om landet inte har en adekvat nivå för skyddet av personuppgifterna. Förbudet gäller också överföring av personuppgifter för behandling i tredje land.

Frågan om en skyddsnivå är adekvat skall bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt skall läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen skall pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredje landet. Lag (1999:1210).

#### *Undantag från förbudet mot överföring av personuppgifter till tredje land*

**34 §** Det är trots förbudet i 33 § tillåtet att föra över personuppgifter till tredje land, om den registrerade har lämnat sitt samtycke till överföringen eller om överföringen är nödvändig för att

- a) ett avtal mellan den registrerade och den personuppgiftsansvarige skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas,
- b) ett sådant avtal mellan den personuppgiftsansvarige och tredje man som är i den registrerades intresse skall kunna ingås eller fullgöras,

- c) rättsliga anspråk skall kunna fastställas, göras gällande eller försvaras, eller
- d) vitala intressen för den registrerade skall kunna skyddas.

Det är också tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter.

#### *Skadestånd*

**48 §** Den personuppgiftsansvarige skall ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med denna lag har orsakat.

Ersättningsskyldigheten kan i den utsträckning det är skäligt jämkas, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne.

#### *Straff*

**49 §** Till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år döms den som uppsåtligen eller av grov oaktsamhet

- a) lämnar osann uppgift i sådan information till registrerade som föreskrivs i denna lag, i anmälan till tillsynsmyndigheten enligt 36 § eller till tillsynsmyndigheten när myndigheten begär information enligt 43 §,
- b) behandlar personuppgifter i strid med 13-21 §§,
- c) för över personuppgifter till tredje land i strid med 33-35 §§,
- d) låter bli att göra anmälan enligt 36 § första stycket eller enligt föreskrifter meddelade med stöd av 41 §,
- e) behandlar sådana personuppgifter som avses i 13 och 21 §§ i strid med 5 a § andra stycket, eller
- f) i strid med 5 a § andra stycket för över personuppgifter till tredje land som inte har en sådan adekvat nivå för skyddet av personuppgifterna som avses i 33 §.

I ringa fall döms inte till ansvar.

Den som överträtt ett vitesföreläggande enligt 44 § eller 45 § första stycket döms inte till ansvar för en gärning som omfattas av vitesföreläggandet. Lag (2006:398).

## Bilaga 3 – Gränsdragningen mellan LEK och PuL

### Sammanfattning

---

#### Slutsats

- LEKs bestämmelser är tillämpliga på operatörens överföring av telefonnummer (identifieringssyfte) och lokaliseringssuppgifter (lokaliseringssyfte).
- Med hänsyn till hur mobiltjänsterna är uppbyggda idag torde huvudregeln vara att PuL är tillämplig på innehållsleverantörens och aggregatörens vidare behandling av dessa uppgifter.

#### Sammanfattande analys

- De uppgifter som i dagsläget överförs från operatörer till mobila innehållstjänster är huvudsakligen telefonnummer och lokaliseringssuppgifter, vilka båda kan kategoriseras som trafikuppgifter.
- De särskilda reglerna om trafikuppgifter i LEK föreskriver att behandling endast får ske av andra aktörer än operatören om denna behandling sker *på uppdrag* av operatören.
- Uttrycket "på uppdrag av" tolkas snävt. Det ska därför bara appliceras på situationer där en operatör lejt ut viss del av verksamheten till en annan part som osjälvständigt utför denna. Detta innebär att bestämmelsen inte torde vara tillämplig på många av de innehållstjänster som återfinns på marknaden, då dessa i de flesta fall levereras av en fristående part som för användaren ger ett självständigt intryck. De särskilda reglerna om trafikuppgifter kan därför generellt inte tillämpas.
- Utöver dessa särskilda regler finns en huvudregel för behandling av samtal och trafikuppgifter som innebär att behandling av trafikuppgifter endast får ske om någon av användarna samtyckt till behandlingen.
- Trots att de särskilda reglerna inte är tillämpliga torde därför operatören med stöd av huvudregeln kunna överföra uppgifter till en utomstående part.
- I sådana fall torde LEK endast omfatta överföringen av uppgifter *från operatören* varefter PuL är tillämplig på den vidare behandling av uppgifter som sker hos aggregatör och/eller innehållsleverantören.

I denna bilaga behandlas frågan om vilken lagstiftning som är tillämplig på behandlingen av uppgifter som utförs av operatörer, aggregatörer respektive innehållsleverantörer. För att kunna avgöra denna fråga är det nödvändigt att först analysera relevanta bestämmelser i LEK.

Analysen inleds med en grundläggande bedömningen av hur de uppgifter som överförs från operatörerna för användning i mobila innehållstjänster ska kategoriseras. Därefter analyseras i vilken utsträckning de särskilda bestämmelser om trafikuppgifter som återfinns i 6 kap. 7 § LEK är tillämpliga på överföringen. Efter en analys av hur huvudregeln om behandling av trafikuppgifter och innehåll, i 6 kap. 17 § LEK, bör tillämpas görs avslutningsvis en bedömning av frågan om gränsen mellan tillämpning av LEK och PuL för den aktuella överföringen av uppgifter.

## **1. Utgör uppgifterna som förs över trafikuppgifter?**

Det är huvudsakligen två typer av uppgifter som överförs från operatörer, till aggregatörer och innehållsleverantörer i samband med att en användare kommunicerar med en mobil innehållstjänst: abonnentens telefonnummer (identifikationssyfte) och mobiltelefonens geografiska position (lokaliseringssyfte). För att kunna bedöma vilka regler som är tillämpliga på behandlingen av dessa uppgifter måste de först kategoriseras.

### Telefonnummer

Som konstaterats ovan i kapitel 2.2 kan ett telefonnummer typiskt sett anses utgöra en abonnentuppgift. Om numret i ett visst sammanhang inte härrör från en samling statiska uppgifter om abonnenten utan snarare utgör en del av de uppgifter som är nödvändiga för att överföra ett elektroniskt meddelande, ska dock uppgiften kategoriseras som en trafikuppgift.

Den information som överförs i det nu aktuella fallet, dvs. i samband med att användare skickar meddelanden till eller begär en viss webbsida från en mobil innehållstjänst, är uppgiften om från vilket telefonnummer de elektroniska meddelandena härrör. Det är alltså en uppgift om avsändaren av elektroniska meddelanden och följaktligen inte huvudsakligen en statisk uppgift om en viss abonnent. Slutsatsen är därför att telefonnumret i detta fall ska anses utgöra en trafikuppgift.

### Lokaliseringsuppgifter

Ovan har även redogjorts för de två kategorier som lokaliseringsuppgifter, beroende på sammanhang, kan tillhöra. Av den information som aktörerna har lämnat till myndigheterna, inom ramen för den genomförda tillsynen, framgår att i de fall lokaliseringsuppgifter inhämtas från operatörer, så rör det sig i dagsläget om sådana uppgifter som behandlas i mobilnäten i syfte att möjliggöra kommunikation med mobiltelefonen. Därav följer att de lokaliseringsuppgifter som behandlas i denna rapport är att betrakta som trafikuppgifter.

## 2. Är de särskilda bestämmelserna om trafikuppgifter tillämpliga?

Efter att ha konstaterat att merparten av de uppgifter som överförs för användning i mobila innehållstjänster utgör trafikuppgifter, är det nödvändigt att avgöra om denna överföring regleras av de särskilda reglerna i LEK om behandling av trafikuppgifter.

Enligt 6 kap. 5 § LEK får en trafikuppgift som avser en viss person, när den inte längre behövs för överföring av ett elektroniskt meddelande eller fakturera ett sådant, inte behållas utan måste utplånas eller avidentifieras. Under förutsättning att abonnenten har samtyckt till detta får dock trafikuppgifter som avser fysiska personer eller abonnenter, enligt 6 kap. 6 § andra stycket LEK, behandlas för att ”tillhandahålla andra tjänster där uppgifterna behövs”. I förarbetena har angivits att detta ska omfatta ”alla tjänster som kräver behandling av trafik- [...] uppgifter utöver vad som är nödvändigt för överföring eller fakturering av en kommunikation.”<sup>9</sup>

PTS har i remissen till LEK menat att trafikuppgifter efter samtycke bör få behandlas även för marknadsföring av andras tjänster. I förarbetena instämmer regeringen i denna slutsats, dock med den begränsning som framgår av artikel 6.3 tillsammans med artikel 6.5 i direktivet om integritet och elektronisk kommunikation.<sup>10</sup> Dessa artiklar begränsar vilka som är behöriga att behandla uppgifterna och har implementerats i 6 kap. 7 § LEK.

I 6 kap. 7 § LEK anges att behandling som utförs efter samtycket får ske ”endast av den som fått i uppdrag av den som bedriver verksamhet som är anmälningspliktig att sköta fakturering, trafikstyrning, kundförfrågningar,

---

<sup>9</sup> Prop 2002/03:110 sid 258

<sup>10</sup> Prop 2002/03:110 sid 258, aktuella artiklar återfinns på sid 492

marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av andra tjänster där uppgifterna behövs”.

Innebörden av kravet på uppdragsförhållande

Frågan är då när någon, inom ramen för 6 kap. 7 § LEK, kan bedömas ha ”fått i uppdrag” att behandla uppgifterna. En jämförelse kan i detta sammanhang göras med formuleringar i artikel 9.1 och 9.3 i samma direktiv. Artiklarna behandlar liknande bestämmelser, avseende lokaliseringssuppgifter som *inte* är trafikuppgifter och har i LEK implementerats i 6 kap. 10 § LEK. I artikel 9.3 anges den behörige att behandla uppgifterna som de ”personer som handlar på uppdrag av leverantören av ett allmänt kommunikationsnät eller en allmänt tillgänglig kommunikationstjänst eller den tredje part som tillhandahåller mervärdestjänsten...”.<sup>11</sup> Detta kan jämföras med nyss nämnda artikel 6.5, som uttrycker den behöriga kretsen som ”sådana personer som av leverantören av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster getts i uppdrag att sköta [...] tillhandahållande av mervärdetjänster...”.<sup>12</sup>

De bestämmelser som har infört de aktuella artiklarna i svensk lag skiljer sig i liknande mån i formuleringen. Lagtexten gör således en skillnad mellan de två bestämmelserna. Enligt 6 kap. 7 § LEK (trafikuppgifter) kan endast den som givits i uppdrag av den anmälningspliktige behandla uppgifterna. Enligt 6 kap. 10 § LEK (lokaliseringssuppgifter som inte är trafikuppgifter) kan behandlingen ske av den som givits i uppdrag av den anmälningspliktige *eller* av den som tillhandahåller den tjänst där uppgifterna behövs.

Mot bakgrund av ovanstående ter det sig som om behandling enligt de särskilda bestämmelserna om trafikuppgifter i 6 kap. 5-7 §§ LEK, får ske för att tillhandahålla andra tjänster (t.ex. en mobil innehållstjänst), endast under förutsättning att den som utför behandling gör det *på uppdrag* av den som är anmälningspliktig (det vill säga tillhandahållaren av den elektroniska kommunikationstjänsten). Om inte ett sådant uppdrag finns, kan behandlingen inte luta sig mot dessa bestämmelser.

Av förarbetena till lagen framgår dock att lagstiftaren anser att oavsett att bestämmelserna om trafikuppgifter och andra lokaliseringssuppgifter är uttryckta på olika sätt torde det i båda fallen vara möjligt att överlåta uppgifter till en tredje part för att denne tredje part ska kunna tillhandahålla tjänster där

---

<sup>11</sup> Prop 2002/03:110 sid 493

<sup>12</sup> Prop 2002/03:110 sid 492

uppgifterna behövs.<sup>13</sup> Detta dock under förutsättning att samtycke om förhållandet föreligger.<sup>14</sup>

Trots skillnaden i formuleringar ter det sig därmed som att lagstiftarens syfte med bestämmelsen är att kretsen av personer som har behörighet att befatta sig med uppgifterna inte ska begränsas endast till dem som erhåller uppdrag direkt av den anmälningspliktige parten.

Mot bakgrund av att formuleringen i bestämmelsen om trafikuppgifter (och direktivet som bestämmelsen bygger på) antyder motsatsen till vad som framgår av förarbetena ter sig rättsläget som oklart. PTS bedömning är därför att hantering inom ramen för uttrycket ”på uppdrag av” måste ses relativt snävt och snarast avse situationer där operatören lejt ut en del av sin egen verksamhet till någon annan som osjälvständigt utför denna verksamhet under operatörens namn.

#### Slutsats

Såvitt PTS kan bedöma stämmer ovanstående kriterier för när en tjänst tillhandahålls ”på uppdrag av” operatören inte väl överens med den föreliggande marknadsstrukturen för majoriteten av fallen där uppgifter förmedlas till mobila innehållstjänster. Det får i normalfallet därför anses förhålla sig så att vare sig aggregatörer eller innehållsleverantörer agerar på uppdrag av operatören i LEKs mening.

PTS slutsats är således att de särskilda bestämmelserna om trafikuppgifter, i 6 kap. 5-7 §§ LEK, i normalfallet inte är tillämpliga på aggregatörens eller innehållsleverantörens behandling. Det ska dock tilläggas att denna slutsats bygger på PTS bedömning av det sätt på vilket flertalet av dagens innehållstjänster torde tillhandahållas.

I vissa fall tillhandahålls dock innehållstjänster genom en av operatören kontrollerad portal, där det för användaren framstår som att tjänsterna tillhandahålls av operatören själv. I praktiken kan även sådana tjänster många gånger tillhandahållas av externa aktörer, trots att de marknadsförs under operatörens varumärke. I dessa fall kan mycket väl kriterierna för ”på uppdrag av” anses vara uppfyllda och behandlingen av trafikuppgifter kan i dessa fall hanteras inom ramen för bestämmelserna i 6 kap. 5-7 §§ LEK. En förutsättning är dock att tillhandahållandet av tjänsten och därmed behandlingen av trafikuppgifter sker osjälvständigt av innehållsleverantören,

---

<sup>13</sup> Prop 2002/03:110 sid 261, jfr även sid 258 där det angående trafikuppgifter hänvisas till sid 261 angående möjligheter att överföra uppgifter till tredje part.

<sup>14</sup> Ang samtycke, se nedan avsnitt 0

som snarast kan sägas agera underleverantör till operatörens egen innehållstjänst. Det bör framgå av såväl avtalet mellan parterna som det faktiska upplägget för uppgiftsbehandlingen att så är fallet. I denna rapport refereras till denna form av innehållstjänst som ”uppdragstjänst”.

### **3. Kan någon annan bestämmelse i LEK tillämpas?**

Även om behandling av uppgifter inte kan ske med stöd av de särskilda bestämmelserna om trafikuppgifter i 6 kap. 5-7 §§ LEK, har det i förarbetena angivits att det torde vara möjligt att, under de förutsättningar som anges i bestämmelserna avseende information och samtycke, överlåta sådana uppgifter till tredje part för att tillhandahålla tjänster där uppgifterna behövs.<sup>15</sup> Det är inte tydligt vad förarbetena bygger denna slutsats på.

Det som enligt PTS bedömning ligger närmast till hands är att istället använda sig av huvudregeln om förbud mot avlyssning som återfinns i 6 kap. 17 § LEK. Där anges bl.a. att trafikuppgifter inte får behandlas på något sätt av någon annan än de användare som utväxlar ett meddelande, om inte någon av dessa användare samtyckt till det. Således innefattar även huvudregeln en samtyckeskonstruktion. Eftersom huvudregeln anges gälla ”utöver vad som anges i 5-7 §§” torde innebörden vara att behandling som hanteras i enlighet med huvudregeln är tillåten även om den inte kan anses omfattas av de särskilda reglerna om trafikuppgifter i 6 kap. 5-7 §§ LEK.

PTS slutsats är därför att den behandling som sker genom överföring av trafikuppgifter till utomstående part, men som inte sker på uppdrag av operatören faller under huvudregeln i 6 kap. 17 § LEK.<sup>16</sup>

### **4. Slutsats om gränsen för tillämpning av LEK**

I normalfallet torde alltså hanteringen vid överföringen av uppgifter *från operatör* till aggregatör eller innehållsleverantör, dvs. kravet på samtycke till sådan behandling, regleras av huvudregeln i 6 kap. 17 § LEK.

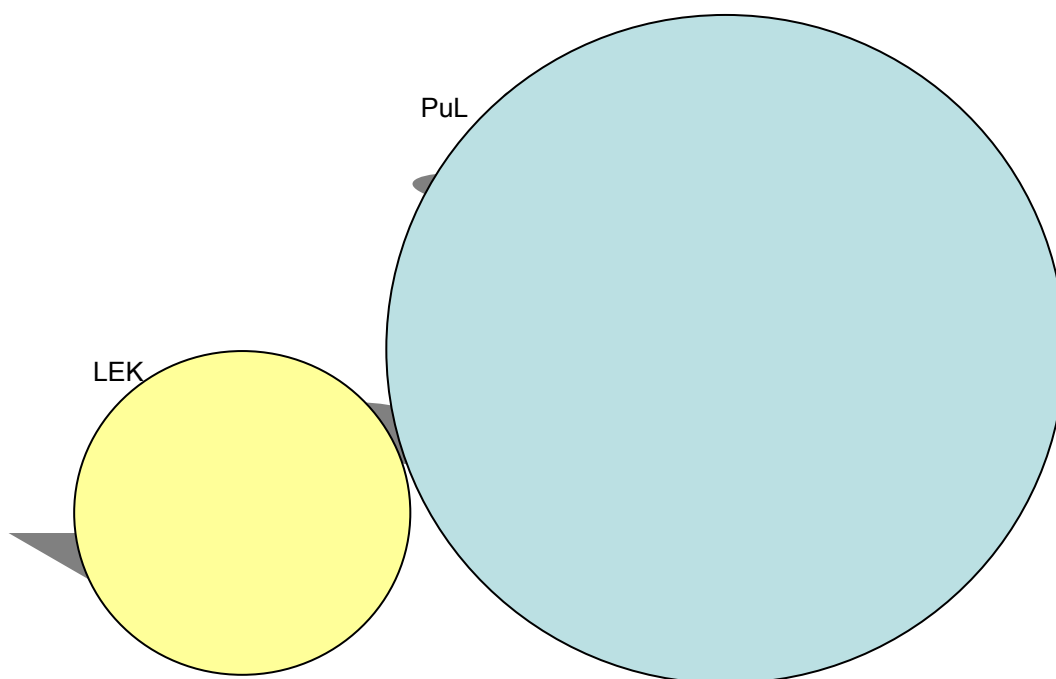
---

<sup>15</sup> Prop 2002/03:110, sid 261

<sup>16</sup> I de fall innehållstjänsterna tillhandahålls som uppdragstjänster under operatörens namn kan dock 6 kap. 5-7 §§ LEK vara tillämpligt.

Den behandling som sker därefter är dock inte lika självklart reglerat i LEK, eftersom regeln endast berör hemligheten av trafikuppgifterna. I normalfallet torde LEK därför endast omfatta överföringen av uppgifter från operatören, varefter PuL får anses tillämplig på den vidare behandling av uppgifterna som sker hos innehållsleverantören. Som jämförelse kan nämnas att operatörers interna hantering av kunduppgifter etc. regleras i PuL medan utlämnandet av sådana uppgifter regleras i LEK (jfr tystnadsplikt och utlämning 6 kap. 20 – 22 §§ LEK).<sup>17</sup>

Figur 3 Förenklad översikt gränsdragning PuL/LEK (normalfallet, enligt 6 kap. 17 § LEK)

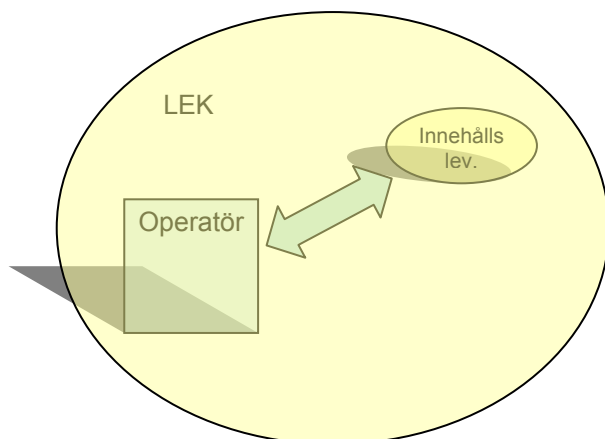


I uppdragsfallet, dvs. de fall där innehållsleverantör agerar på uppdrag av operatören, tillämpas däremot 6 kap. 7 § LEK. LEK är i detta fall tillämpligt på hela kedjan av behandling och PUL ska således inte tillämpas.

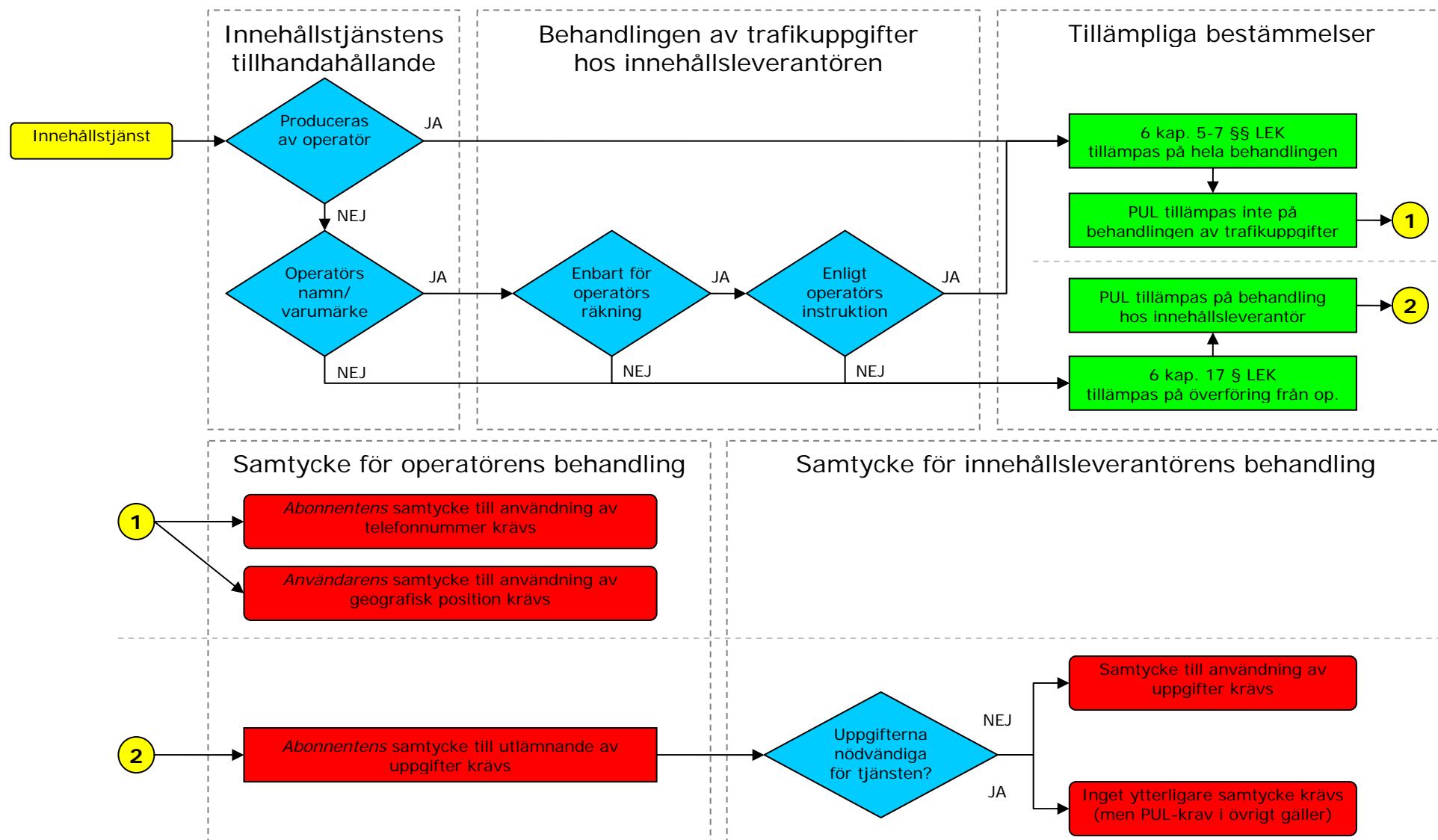
---

<sup>17</sup> I de fall innehållstjänsterna tillhandahålls som uppdragstjänster under operatörens namn är dock 6 kap. 5-7 §§ LEK tillämplig på hela kedjan av aktörer, PUL blir således inte tillämpligt på behandlingen av trafikuppgifter vid tillhandahållandet av innehållstjänsten i dessa fall.

Figur 4 Förenklad översikt (uppdragsfallet, enligt 6 kap. 7 § LEK)



## Bilaga 4 – Schematisk bild över gränsdragningen mellan LEK och PuL



## Bilaga 5 - Tekniska begrepp

**GSM** (Global System For Mobile Communication) är den tekniska standard som används för den andra generationens mobiltelefoni.

**GPRS** (General Packet Radio Service) är en teknik för mobil överföring av data.

**UMTS** (Universal Mobile Telecommunications System) är den av den tredje generationens mobilkommunikationstekniker som är vanligast i Sverige.

**HTTP** (Hyper Text Transfer Protocol) är ett kommunikationsprotokoll som används för att överföra webbaserat material till en webbläsare i t.ex. en dator eller mobiltelefon.

**HTTPS** (Hyper Text Transfer Protocol Secure) är en vidareutveckling av http, som förser överföringen med kryptering. HTTPS används ofta vid inloggning till Internettjänster, i syfte att skydda användarnamn och lösenord mot otillbörlig insyn.

**VPN** (Virtual Private Network) innebär att en s.k. virtuell tunnel upprättas mellan två punkter i nätverket, genom vilken information kan överföras krypterat.

**WAP** (Wireless Application Protocol) är en protokolluppsättning som har utvecklats med särskilt beaktande bl.a. av mobila enheter, som handdatorer och mobiltelefoner, som har begränsad processorkraft, minne och skärmyta. WAP-tekniken gör det möjligt att ta del av tjänster och information på Internet, i en mobiltelefon.