Myndigheters outsourcing av personuppgiftsbehandling i molntjänster

Särskilt om legalitetsprincipen och personlig integritet

Robin Pettersson

Examensarbete i rättsinformatik, 30 hp
Examinator: Stanley Greenstein
Stockholm, Vårterminen 2018
Abstract

This thesis examines the legal means by which the Swedish government authorities can outsource personal data to be processed on digital clouds by private cloud providers as of May 25th, 2018. The objective of the thesis is to identify and examine to which extent legal obstacles and restrictions to such procedures occurs in the personal data protection regulation.

Cloud computing is an information technology business model which could provide government authorities with higher administrative efficiency and lower administrative costs. The essential characteristics of cloud computing require that the cloud providers are entrusted with a portion of control of the IT-environment and data security, depending on the types of clouds and services provided.

The thesis analyses particularly two questions. The first question is to which extent the legal requirement to provide personal data with an appropriate level of security constrains government authorities to submit control of the IT-environment to private contractors. The second question targeted in the thesis is whether government authorities can disclose personal data that is subjected to official secrecy to the cloud providers.
Förkortningar

GDPR Europaparlamentets och rådets förordning 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG

Dataskyddsdirektiv 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 (General Data Protection Regulation)

DI Datainspektionen
CSA Cloud security alliance
EDPS Europeiska datatillsynsmannen (European Data Protection Supervisor)
EKMR Europeiska konventionen den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna
ENISA The European Network and Information Security Agency
eSam E-samverkansprogrammet
EU Europeiska unionen
FEU Fördraget om Europeiska unionen
FEUF Fördraget om den Europeiska unionens funktionssätt


Förslag till ny myndighetsdatalag Förslag till myndighetsdatalag SOU 2015:39 s. 37.

Förslag till ny svensk dataskyddsförordning Förslag till förordning med kompletterande bestämmelser till Europeiska unionens dataskyddsförordning SOU 2017:39 s. 55.

IaaS Infrastructure as a service
ITO Informationsteknisk outsourcing
JO Justitieombudsmannen
MSB Myndigheten för samhällsskydd och beredskap
NIST National Institute of Standards and Technology
OSL Offentlighets- och sekretesslagen (2009:400)
PaaS Platform as a service
Prop. Regeringens proposition till riksdagen
PuL Personuppgiftslag (1998:204)
RF Regeringsform (1974:152)
Rättighetsstadga Den Europeiska unionens stadga om de grundläggande rättigheterna
SaaS Software as a service
SIS Swedish Standards Institute
SOU Statens offentliga utredningar
WP29 Arbetsgruppen för skydd av personuppgifter instiftad genom artikel 29 i 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 (The Data Protection Working Party established by Article 29 of Directive 95/46/EC)
INNEHÅLLSFÖRTECKNING

1 Inledning .......................................................................................................................... 5
  1.1 Om ämnet ....................................................................................................................... 5
    1.1.1 Molntjänster och legalitet ...................................................................................... 5
    1.1.2 Molntjänster och personlig integritet ...................................................................... 6
    1.1.3 Ämnets plats i rättssystemet ................................................................................... 6
    1.1.4 Ämnets plats i molntjänstaffärer ........................................................................... 7
  1.2 Syfte och frågeställning ............................................................................................... 7
  1.3 Avgränsningar ............................................................................................................. 8
  1.4 Material ......................................................................................................................... 9
  1.5 Metod ............................................................................................................................ 11
    1.5.1 Rättsdogmatisk metod och rättsanalytisk metod .................................................... 11
    1.5.2 Juridisk metod ........................................................................................................ 12
  1.6 Disposition .................................................................................................................... 13

2 Molntjänster ...................................................................................................................... 13
  2.1 Om molntjänster ........................................................................................................... 13
    2.1.1 Om beteckningen molntjänster ............................................................................. 14
    2.1.2 Om definitionen av molntjänster ......................................................................... 14
  2.2 Vad är molntjänster? ...................................................................................................... 15
    2.2.1 Molntjänstens fem essentiella kännetecken .......................................................... 15
    2.2.2 Molntjänsters tre tjänstemodeller ......................................................................... 16
    2.2.3 Molntjänster fyrar leveransmodeller ..................................................................... 16
  2.3 Molntjänster och outsourcing ..................................................................................... 17
    2.3.1 Vad är outsourcing? ............................................................................................... 17
    2.3.2 År molntjänstavtal outsourcing? ........................................................................... 17
  2.4 Statistik ......................................................................................................................... 18
  2.5 Sammanfattning ............................................................................................................ 19

3 Överblick av integritetsskyddsregleringen ....................................................................... 20
  3.1 Integritetsskyddsregleringen och reglerna i en generell och speciell del ..................... 20
  3.2 Integritetsskydd och rättssystemets normativa hierarki .............................................. 21
  3.3 Internationella åtaganden avseende integritetsskydd .................................................. 22
  3.4 Integritetsskydd inom den Europeiska unionens primärstrakt ................................... 23
  3.5 Integritetsskydd i grundlagen ...................................................................................... 24
  3.6 Den allmänna dataskydds förordningen (GDPR) .......................................................... 24
  3.7 Offentlighets- och sekretesslagen ............................................................................. 26
  3.8 Förslaget till ny dataskydds lag och ny svensk dataskydds förordning .................... 26
  3.9 Sammanfattning ........................................................................................................... 27

4 Personuppgifter och myndigheters ansvar ......................................................................... 28
  4.1 Vad betyder personuppgifter? ....................................................................................... 28
    4.1.1 Personuppgifters fyra beståndsdelar ...................................................................... 29
    4.1.2 Beståndsdelens ”varje upplysning” ....................................................................... 29
    4.1.3 Beståndsdelens ”som avser en” ........................................................................... 29
    4.1.4 Beståndsdelens ”identifierad eller identifierbar” .................................................. 30
    4.1.5 Beståndsdelens ”fysisk person” ............................................................................. 30
    4.1.6 Ett juridiskt verktyg vid bedömningen ................................................................. 30
  4.2 Vad betyder personuppgiftsansvar? ............................................................................. 31
  4.3 Vad betyder personuppgiftsansvar? ............................................................................. 31
  4.4 Hur kan myndigheter underkastas personuppgiftsansvar? .......................................... 32
    4.4.1 Registerförfattningarna ......................................................................................... 32
    4.4.2 Personuppgiftsansvarets tre beståndsdelar .......................................................... 33
    4.4.3 Beståndsdelens ”bestämmer ändamål och medlen” .............................................. 33


4.4.4 Beståndsdel "en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ". 33
4.4.5 Beståndsdel "som ensamt eller tillsammans med andra". 34

5 Allmänt om laglighetsprövningen. 36
5.1 Laglighetsprövning och lämplighetsprövning. 36
5.2 Klarläggande av omständigheter. 36
5.3 Laglighetsprövningens omfattning. 37
5.4 Direkta och indirekta legala hinder. 38
5.5 Legala utmaningar. 38
5.6 Sammanfattning. 38

6 Personuppgifternas säkerhetsnivå. 39
6.1 Kravet på lämplig säkerhetsnivå. 39
6.2 Konkreta åtgärder som höjer säkerhetsnivån. 40
6.3 Bedömning av lämplig säkerhetsnivå.
   6.3.1 Risk- och sårbarhetsanalys. 42
   6.3.2 Informationsklassificering. 43
6.4 Lämplig säkerhetsnivå och olika molntjänster. 44
6.5 Sammanfattning. 46

7 Överlämnande av personuppgifter. 48
7.1 Personuppgifter utan sekretess. 48
7.2 Innebörden av sekretess. 49
7.3 Sekretessprövning. 49
7.4 Schabloniserad sekretessprövning. 50
7.5 Nödvändigt för att fullgöra myndighetens verksamhet. 51
7.6 förbehåll om tystnadsplikt. 53
7.7 Molntjänster utan att röja uppgifterna? 53
7.8 Personuppgifter som rör hälsa. 55
7.9 Personuppgifter som rör lagöverträdelser. 55
7.10 Sammanfattning. 56

8 Avslutande reflektioner. 57
1 INLEDNING

Marknaden för molntjänster växer kraftigt. Vissa uppskattningar indikerar att den europeiska molntjänstmarknaden kommer att nästan femdubblas till en omsättning på strax under 50 miljarder svenska kronor mellan år 2013 och 2020.¹ Molntjänster håller på att gå från ett sätt man kan arbeta med IT på, till det sättet man arbetar med IT på.

Molntjänster innebär att hård- och mjukvara allokeras till leverantören. Detta möjliggör för ett utnyttjande av stordriftsfördelar som skapar en effektivare resursanvändning. Kunderna kan på det sättet övriga mer ansvar för drift och underhåll till leverantörerna samtidigt som de endast betalar för den IT de faktiskt använder.

Den svenska förvaltningen har inte försuttit chansen att nyttja fördelarna som molntjänster för sig. Enligt en enkätundersökning utförd år 2015 av Pensionsmyndigheten använde åtminstone 78% av de 148 svarande myndigheterna molntjänster i sina respektive verksamheter.² Detta relativt nya sätt för myndigheter att bedriva IT på ger upphov till nya typer av juridiska utmaningar gällande bland annat legalitet och personlig integritet.


1.1 OM ÄMNET

1.1.1 Molntjänster och legalitet

Legalitetsprincipen är en grundbult i det svenska statsskicket och innebär att alla åtgärder vidtagna med det offentligas makt måste ha stöd i en lagregel. Princinen återfinns i 1 kap. 1 § 3 st. regeringsformen [RF] under lydelsen ”[d]en offentliga makten utövas under lagarna”.

I det moderna digitaliserade samhället uppkommer nya typer av utmaningar för att bibehålla kontrollen över den offentliga verksamheten. Informationsteknologin skapar effektiviseringsmöjligheter som kan underlätta såväl myndigheternas arbetsbörda som skattebetalarnas finansiella bördas. Strävanheten efter en effektivisering av förvaltningen får emellertid inte ensamt vara skäl nog för myndigheter att hemfalla åt de lösningar som marknaden erbjuder. Oavsett hur rationella molntjänster är för myndigheters ur effektivitetsynpunkt får de inte användas om det inte finns stöd för detta genom lag. Kontrollen över den offentliga verksamheten är nämligen ett grundläggande attribut hos en rättsstat.³

Samtidigt som molntjänster redan används i förhållandevis stor utsträckning inom den statliga förvaltningen berättar många myndigheter i Pensionsmyndighetens enkätundersökning att de upplever en juridisk osäkerhet rörande molntjänster.⁴ Det föreligger sålunda ett behov av ökad juridisk klarhet

² Pensionsmyndigheten, Molntjänster i staten, s. 15.
³ Se KU 1973:26 s. 59 där konstitutionsutskottet uttryckt att denna bestämmelse i själva verket ger uttryck för principen att Sverige är en rättsstat.
⁴ Pensionsmyndigheten, Molntjänster i staten, s. 37.
vilket motiverar en närmare utredning av de legala förutsättningarna för myndigheters användning av molntjänster.

1.1.2 Molntjänster och personlig integritet
Trots att personlig integritet erkänds som en grundläggande mänsklig rättighet finns ingen allmänt erkänd definition om vad personlig integritet egentligen innebär. Ofta beskrivs dock den personliga integriteten som en enskilds rätt till skydd av sin personliga sfär, att bli lämnad i fred eller att få bli bortglömd på Internet.\(^5\)

Digitalisering skapar större möjligheter för myndigheter att bland annat samla och söka i uppgifter om enskilda. Ofta besitter myndigheter mycket information som är integritetskänslig. För att skydda enskildas rätt till personlig integritet är det därför av vikt att informationen hålls säker och oåtkomlig för obehöriga. Förvaltningens användning av privata leverantörs molntjänster innebär att den privata sektorn spelar en större roll i vid informationssäkerhetsarbetet. Centraliseringen av data skapar också nya typer av säkerhetsmässiga utmaningar i strävandet efter att värna enskildas rätt till personlig integritet.

Integritetsskyddslagstiftningen står inför stora förändringar. Under en övergångsperiod medför större legala reformer ofta ökad risk för oförutsebar och osäker tillämpning av reglerna. Teoretiska framställningar av analyserande slag kan bidra till att mildra de risker som uppstår vid sådana reformer. Denna situation motiverar att uppsatsens utredning inriktas på att analysera de legala förutsättningarna för myndigheters användande av privata leverantörs molntjänster i förhållande till kraven på enskildas grundläggande rätt till personlig integritet.

1.1.3 Ämnets plats i rättssystemet
För överblickens skull ska uppsatsens ämne placeras i sitt sammanhang i det juridiska rättssystemet. Detta görs med användande av den traditionella uppdelen av rätten i två huvudkategorier. Den första av dessa kategorier är civilrätt, till vilken regler om förhållandet mellan privata aktörer hör. Underkategorier till civilrätten är till exempel avtalsrätt, familjerätt och associationsrätt vilka i sin tur innehåller subkategorier av rättsregler.

Den andra huvudkategorin är offentlig rätt vilken i motsats till civilrätten består av sådana normer som reglerar det allmäna och dess förhållande till privata aktörer. Underkategorier till offentlig

\(^5\) Magnusson Sjöberg m.fl. s. 149 f.
rätt är till exempel straffrätt, skatterätt, statsrätt och förvaltningsrätt.


1.1.4 Ämnets plats i molntjänstförrådet
Molntjänststaffärer mellan myndigheter och leverantörer kan delas upp i tre huvuddelar bestående av identifikation av avtalspart, förhandling av avtalsvillkor och verkställande av avtalet. Den här uppsatsen handlar om en del av avtalsförhandlingen. En jurists roll i en sådan förhandling är dels att bestämma affären yttre gränser, dels att strukturera affären så att den blir så bra som möjligt för klienten inom ramen för dessa gränser. De yttre ramarna för affären utgörs av fyra olika typer av begränningar, nämligen vad som är tekniskt, finansiellt och juridiskt möjligt samt vad som är möjligt för en part att efterleva. De legala begränsningarna i ett molntjänstavtal är många och innefattar ofta frågor om till exempel immaterialrätt, sekretess, ansvar och personuppgifter. Uppsatsen syftar till att utreda och analysera de legala begränsningarna i molntjänstavtal som kan härledas till personuppgiftsfrågor, särskilt avseende informationssäkerhet och integritetsskydd.

1.2 Syfte och Frågeställning
Det konkreta syftet med uppsatsen är att undersöka och analysera vilka legala hinder som i integritetsskydds lagstiftningen av den 25 maj 2018 begränsar myndigheters från att ingå affärsämne outsourcingavtal om molntjänster med privata aktörer med anledning av att informationen i molntjänsterna utgörs av personuppgifter. Syftet har valts med anledning av att den kraftiga ökningen av användandet av molntjänster i kombination med de förestående förändringarna inom integritetsskydds lagstiftningen torde ha lett till ett ökat behov av orienterande material inom ämnet. Datumet 25 maj 2018 har bestämts med anledning

---

6 Strömberg & Lundell s. 22.
av att svenska domstolar då ska börja tillämpa GDPR. I samband med detta planeras även förändringar i nationell lagstiftning.


Det övergripande syftet med alla rättsvetenskapliga undersökningar är att öka rättssäkerheten och förutsebarheten i rättslivet. En enskild uppsats gör i bästa fall en marginell skillnad i det avseendet. För att det övergripande syftet inte ska gå förlorat är det viktigt att uppsatsen rör rättsregler som på något sätt är angelägna för samhället. Myndigheter måste redan idag inställa sig efter det framtida rättsläge som inträder efter att förändringarna inom integritetsskyddslagstiftningen börjar tillämpas. En analys som beaktar dessa förändringar gör sig därför mer relevant än en rättsdogmatisk utredning av gällande rätt.

Det praktiska syftet med uppsatsen är att läsaren ska kunna använda sig av framställningen vid en pågående eller planerad användning av molntjänster för personuppgiftsbehandling för att informera sig om dess analyser och slutsatser. Uppsatsen bör kunna användas som ett proaktivt verktyg för att orientera sig om vilka huvudsakliga integritetsaspekter som gör sig gällande i dessa situationer.

### 1.3 Avgränsningar


Många myndigheters personuppgiftsbehandling är föremål för specialreglering i de så kallade registerförfattningarna. Det är dock främst den generella delen av integritetsskyddsregleringen som är föremål för den förestående förändringen och där riskerna för övergångseffekter är som störst. Registerförfattningarna har föreslagits få fortsatt företräde framför den generella integritetsskyddsregleringen inom gränsen för vad som utgör nationella angelägenheter och den förestående reformen kommer därför inte medföra någon rättslig förändring i de delarna. Vad gäller de regler i registerförfattningarna som faller inom unionsrättens gränser har GDPR företräde i enlighet med principen om Europeiska unionsrättens företräde. Gränsen mellan unionsrätt och nationell rätt och dess betydelse för tillämpningen av registerförfattningarna är i och för sig en intressant fråga men behandlas inte i den här uppsatsen.

---

7 Se kapitel 1.4 “Material” för en närmare beskrivning av GDPR.
8 Korling & Zamboni, s. 27.
9 GDPR art. 99(2).

1.4 MATERIAL

I uppsatsen har traditionellt juridiskt källmaterial använts. Som ovan beskrivits står dock det juridiska materialet inom integritetsskyddsområdet inför förändringar. Eftersom analysen rör ett framtidigt rättsläge av ett datum som efterträder stora förändringar inom den nuvarande integritetsskydds- lagstiftningen har även annat material än det traditionella juridiska källmaterialet fått beaktas vid ut tolkningen av det framtida rättsläget. Dessa källor omfattar bland annat beslut, rapporter, faktablad, enkäter och allmänna rekommendationer från svenska och europeiska offentliga organ och förslag till ny lagstiftning. Även rapporter och vägledningar från ideella organisationer och utländska myndigheter har använts i analysen. Allt material som inte kan härledas till de traditionella rättskällorna har tolkats med försiktighet och tillfogats noggranna hänvisningar. Nedan beskrivs i detalj vilket material som använts i uppsatsen och vilket värde det materialet har getts i analysen.


10 Prop. 2017/18:105, s. 15.
11 GDPR, art. 94(1).
12 SOU 2017:39 s. 78.
målet. Försiktighet måste emellertid påkallas i dessa situationer eftersom det kan vara svårt att av-göra huruvida rättsläget faktiskt har förändrats eller inte. Rättsläget kan av olika skäl förändras trots att ordalydelsen i bestämmelsen är densamma som i en tidigare rättsakt.

Samtliga rättsfall som används i arbetet har värderats under arbetets gång med användande av sedan-vanlig juridisk metod och prejudikatvärdering. Hänvisningar till rättsfall görs bara i de fall dessa använts som referenser i analysen. Uppsatssens analys omfattar alla rättsfall från både prejudicerande domstolar och underinstanser, vilka berör temat integritetsfrågor i förhållande till myndigheters användande av molntjänster.

Samtliga tillsynsbeslut från Datainspektionen vilka rör temat integritetsfrågor i förhållande till myndigheters användande av molntjänster har granskats under arbetets gång. Detta gäller även alla tillsynsbeslut av Justitieombudsmannen [JO] som rör samma tema och som JO själv ansett vara av särskilt intresse.

I arbetet används två olika lagförslag och ett förslag till ny svensk förordning. Dessa tre är förslaget till ny lag med kompletterande bestämmelser till Europeiska unionens dataskyddsförordning13 [förslaget om ny dataskyddslag], förslaget till ny förordning med kompletterande bestämmelser till Europeiska unionens dataskyddsförordning14 [förslaget om ny svensk dataskyddsförordning] och förslaget till ny myndighetsdatalag [förslaget till ny myndighetsdatalag15].


---

13 Prop. 2017/18:105, s. 7.
14 SOU 2017:39, s. 55.
15 SOU 2015:39, s. 37.
16 I samband med att GDPR träder ikraft kommer WP29 att ersättas av ett nytt rådgivande organ under Europeiska Unionen vid namn Europeiska datatillsynsmannen.
utgör soft law och har använts i uppsatsens analys. Dessa källor har alltid tillfogats noggranna hänvisningar.

Som tidigare påpektats rör uppsatsen ett förhållandevis nytt fenomen i samhället. Många är ännu inte bekanta med hur teknologin bakom molntjänster fungerar ens på ett abstrakt plan. En del av uppsatsen har därför vigs åt att förklara vad molntjänster är. Någon beskrivning av de teknologiska detaljerna står dock inte att finna i de traditionella rättskällorna varför annat material har fått användas i förklarande syfte.

1.5 Metod

1.5.1 Rättsdogmatisk metod och rättsanalytisk metod


Ytterligare två skillnader mellan rättsdogmatisk metod och rättsanalytisk metod är med vilken litterär frihet texten produceras och vilket underlag som används. Den rättsdogmatiska argumentationen är sträng och bunden till de allmänt erkända rättskällorna. Den rättsanalytiska metoden och andra sidan tillåter att texten leds av öppet redovisade värderingar eller infallsvinklar.

17 Korling & Zamboni, s. 24 och s. 27.
18 Korling & Zamboni, s. 26.
19 Korling & Zamboni, s. 27 f.
20 Korling & Zamboni, s. 21.
21 Angående denna diskussion se Sandgren, s. 45 ff.
I den här uppsatsen används material utanför de traditionella rättskällorna. Uppsatsen präglas dock inte av någon tes eller särskild värdering eller infallsvinkel. Argumentationen hålls istället, när så är möjligt, i nära förbindelse med de principer som gäller för rättsdogmatisk metod.

1.5.2 Juridisk metod


22 Korling & Zamboni, s. 21.
1.6 Disposition

Uppsatsens analys inleds i kapitel två med en bakgrund kring molntjänster som fenomen. I denna del beskrivs molntjänster i förhållande till både juridik och teknik eftersom en grundläggande kunskap bakom tekniken i molntjänster är en förutsättning för förståelsen av den fortsatta analysen. Kapitlet avslutas med ett avsnitt om hur molntjänster används i den offentliga förvaltningen i praktiken.

Integritetskyddslagstiftningen är svåröverskådligt, dels för att det juridiska materialet spänner över alla normnivåer, dels för att det står inför betydande förändringar. Det tredje kapitlet syftar till att orientera läsaren i materialet och ge en bakgrund till rättssområdet.


I det femte kapitlet analyseras hur myndigheter bör förfara för att ta reda på om de lagligen kan anlita privata molntjänstleverantörer för personuppgiftsbehandling i en viss situation. I kapitlet identifieras vilka typer av legala utmaningar och hinder som aktualiseras. I synnerhet aktualiseras två typer av hinder, vilka utreds närmare i kapitel sju och åtta.

Det sjätte kapitlet bygger vidare på analysen i det sjätte kapitlet men krymper fokusområdet i analysen till att röra just vilka hinder som kan uppstå med anledning av kraven på vilken säkerhetsnivå som ska omgärdas personuppgifter. En beskrivning ges av hur myndigheter bör gå tillväga för att bedöma vilken säkerhetsnivå som krävs och vilka konsekvenser det får för frågan huruvida myndigheter kan behandla personuppgifter i molntjänster.

I det sjunde kapitlet växlas fokusområdet över till den andra typen av hinder som identifierades i kapitel fem. Frågan rör vilka hinder som sektesslagstiftningen medför vid myndigheters outsourcing av personuppgiftsbehandling i molntjänster. Efter en undersökning av vilka krav som uppställs analyseras vad de har för följd för myndigheters möjligheter att behandla personuppgifter i molntjänster.

I uppsatsens åttonde kapitel ges slutligen några egna reflektioner som uppstått under arbetets gång.

2 Molntjänster

2.1 Om molntjänster


23 CD-ROM är en akronym för det engelska uttrycket ”compact disc read only memory”.

2.1.1 Om beteckningen molntjänster
Fenomenet molntjänster beskrivs ofta även med andra termer, till exempel digitala moln, IT-moln, datormoln, molnbaserade datortjänster eller cloudtjänster. Molntjänster torde dock idag ha kommit att bli den vanligaste beteckningen. Förr i tiden, när Internet fortfarande var obevänt för många människor, användes ordet ”moln” som en metafor för att beskriva nätverk och webbsidor. Idag används termen dock som en metafor för en affärsmodell, vilken ska beskrivas närmare nedan.


2.1.2 Om definitionen av molntjänster
WP29 definierar molntjänster i ett av sina uttalanden på följande vis “Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. Cloud computing can generate important economic benefits, because on-demand resources can be configured, expanded and accessed on the Internet quite easily. Next to economic benefits, cloud computing may also bring security benefits; enterprises, especially small-to-medium sized ones, may acquire, at a marginal cost, top-class technologies, which would otherwise be out of their budget range.”

Myndigheten ”European Data Protection Supervisor” [EDPS] kommer i samband med att GDPR blir tillämplig i medlemsstaterna överta WP29:s uppgift att rådge medlemsstaternas och unionens lagstiftare. EDPS beskriver molntjänster på följande sätt ”Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand. It is a paradigm shift following the shift from mainframe to client–server in the early 1980s. Cloud computing describes a new consumption and delivery model for IT services based on the Internet, and it typically involves the provision of dynamically scalable and often virtualised resources as a service over the Internet. It is a by-product and consequence of the ease-of-access to remote computing sites provided by the Internet.”

Swedish Standards Institute [SIS] är en organisation som arbetar med standardisering på många olika områden. Organisationen är representant för Sverige i dess internationella motsvarigheter European Committee for Standardization och den globala Internationella standardiseringsorganisationen. SIS definierar molntjänster som ”ett koncept som möjliggör nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser som via självbetjäning levereras och administreras på begäran.”

---

24 Cloud Sweden, Molnet i offentliga sektorn, s. 4.  
26 Europeiska datatillsynsmannen, Glossary, ”https://edps.europa.eu/node/3098#cloudcomputing”.  
Inte heller Förenta staternas lagstiftning innehåller någon legaldefinition för molntjänster. Där har emellertid en myndighet med namnet ”National Institute of Standards and Technology” [NIST] gett ut en rekommendation som innehåller en utförlig och teknisk beskrivning av molntjänster. NIST-definitionen av molntjänster har fått stor spridning och betydelse för molntjänstmarknaden. NIST-definitionen lyder enligt följande ”Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources --- that can be rapidly provisioned and released with minimal management effort or service provider interaction.” NIST har till denna beskrivning fogat fem essentiella kännetecken för molntjänster och kategoriserat dem i olika typer av tjänste- och leveransmodeller. Dessa modeller beskrivs i detalj nedan.

De olika ansatserna att definiera molntjänster förenar sig kring att molntjänster innebär leverans av delade IT-resurser över nät, oftast via Internet, vilka levereras på begäran. Resurserna ska vara elastiskt skalbara, eller åtminstone med lättethet kunna konfigureras över nätet. SIS och NIST betonar även att molntjänster kännetecknas av självbetjänning eller åtminstone minimal interaktion mellan molntjänstleverantör och kund. Det finns många fler förslag på hur molntjänster bör definieras, inte minst bland molntjänstleverantörerna. Redan av de här redovisade förslagen kan dock konstateras att molntjänster ska förstås som en affärsmodell snarare än en typ av teknologi.

NIST-definitionen är det kanske mest genomarbetade förslaget med hänsyn till dess tekniska detaljbeskrivning. Det är dock viktigt att beakta att ju mer specificerad beskrivningen är desto större chans att definitionen förr eller senare blir obsolet på grund av fortsatt teknisk utveckling. Vilken definition molntjänster ges kan ha betydelse i juridiska sammanhang, till exempel vid marknadsförings- och avtalsfrågor. Trots att definitionen av molntjänster är en pågående diskussion fungerar NIST-definitionen väl när man talar om molntjänster i såväl tekniska som juridiska sammanhang. NIST-definitionen fungerar även väl för att besvara frågeställningen i den här uppsatsen och kommer därför att fungera som grund till begreppet i den fortsätta framställningen. I samband med NIST:s ansats att definiera molntjänster kategoriseras även molntjänster utifrån typ av tjänstemodell och leveransmodell. NIST-definitionen och dess kategoriseringar beskrivs utförligt i de följande avsnitten.

2.2 Vad är molntjänster?

2.2.1 Molntjänsters fem essentiella kännetecken
Det första av de fem kännetecknen är att tjänsten ska vara tillgänglig för självbetjänning på begäran (on-demand self-service), vilket innebär att en användare ensidigt kan bestämma sig för att använda tjänsten utan att automatiskt behöva interagera med en annan människa. Tjänsten ska också ha bred tillgänglighet via nätverk (broad network access) vilket innebär att det ska vara möjligt att komma åt tjänsten genom ett stort nätverk, till exempel Internet. Det tredje kännetecknet är att tjänsten konserverar resurser (resource pooling) vilket innebär att leverantören levererar tjänsten till fler än en användare. Det ska finnas en typ av lokaliseringsjävståndighet som innebär att användaren normalt inte har kontroll eller vetskap om var informationen finns annat än på en mer abstrakt nivå till exempel i vilket land eller i vilken datahall. Det fjärde kännetecknet är att tjänsten ska ha en snabb elasticitet (rapid elasticity) innebärande att dataförmågan skalas upp respektive ned på ett automatiskt, eller åtminstone elastiskt, sätt i förhållande till användarens efterfrågan vid just den stunden. För

28 Recommendations of the National Institute of Standards and Technology, U.S. department of commerce, Special Publication 800-145, September 2011 [cit. NIST].
29 Pensionsmyndigheten, Molntjänster i staten, s. 10.
30 Magnusson Sjöberg m.fl. s. 206.
31 Magnusson Sjöberg m.fl. s. 443.
användaren framstår det normalt som att datakraften nästan är obegränsad. Det femte och sista kännetecknet är att tjänsten ska erbjuda betalning efter användning (measured service) vilket innebär att molnsystemet automatiskt kontrollerar och optimerar resursanvändningen i förhållande till användarens behov. Detta kan till exempel ske genom att användaren betalar för tjänsten till den mängd eller antal som tjänsten ska eller redan har använts. Detta kännetecken har kallats ibland för ”IT på kran” som en metaforisk anspelning på hur man i hushållet betalar för sådan vattenförbrukning som sker genom att man spolar med vattenkranarna. Man behöver inte betala för mer IT än man förbrukar eftersom man kan ”vrida åt kranen” när man är klar.

2.2.2 Molntjänsters tre tjänstemodeller
Molntjänster kategoriseras i tre olika typer av tjänster. Denna kategorisering av molntjänster kallas för SPI-modellen. SPI står för den först skrivna bokstaven i förkortningarna SaaS, PaaS och IaaS, vilkas innebörd förklaras nedan i detta avsnitt. Modellerna skiljer sig främst åt genom att de förser användaren med olika grader av kontroll över tjänsten.


Med tjänstemodellen platform as a service (PaaS) erbjuder leverantören, utöver vad som gäller för IaaS, sådan programvara som användaren kan nytta för att skapa eller använda egna applikationer. Den programvaran kan bestå av programmeringsspråk, bibliotek och vissa andra typer av tjänster eller applikationer.

Modellen software as a service (SaaS) innebär störst ansvar för leverantören av de tre modellerna. Genom SaaS-tjänster erbjuder leverantören inte bara infrastrukturen utan även programvara och applikationer som användaren kan nytta.

2.2.3 Molntjänsters fyra leveransmodeller
Utöver de tre olika typerna av tjänstemodeller som beskrivs i avsnittet ovan finns fyra olika typer av leveransmodeller. En molntjänst har alltid en typ av tjänstemodell och en typ av leveransmodell. De olika modellerna kan kombineras med varandra på vilket sätt som helst för att överföra ett större eller mindre ansvar till leverantören.

över hårdvaran. Det är sålunda en öppen avtalsfråga hur ansvaret för till exempel drift, underhåll och personal ska fördelas.\textsuperscript{32} Med privata moln finns goda möjligheter att anpassa säkerhetsnivån utifrån kundens specifika behov. Kunden kan med privata moln behålla en större direkt kontroll över IT-miljön än vad som är möjligt med de andra leveransmodellerna.

Gemensamma moln fungerar på samma sätt som privata moln med den skillnaden att det finns flera kunder som delar på ett moln. För att denna leveransmodell ska vara att föredra framför övriga modeller krävs att kunderna i fråga har någonting gemensamt, till exempel likartade verksamheter eller säkerhetskriter. Det är endast när kundgruppen har likartade behov som en exklusiv leverans för just den gruppen medför ekonomiska och praktiska fördelar. Även vid gemensamma moln är det en öppen avtalsfråga hur ansvaret för datahallens drift, säkerhet, ägande, lokaliserings och kapitalinvestering med mera ska fördelas.\textsuperscript{33}

I publika moln erbjuds allmänheten att nytta tjänsten varför ägandet av och ansvaret för datorhallen ankommer på leverantören. Detta är den vanligaste formen av molntjänster bland slutkonsumenter.\textsuperscript{34} Detta leveranssätt minskar möjligheterna för kunder att ha hög kontroll på IT-miljön, lagrad data, geografiska lokaliserings, fysiska säkerhet och på driftsäkerheten. Vid publika moln finns sällan möjlighet för leverantörer att överlåta ansvar för till exempel drift, personal och andra säkerhetsrelaterade aspekter av molntjänsten till en viss kund. Kunden har därför små möjligheter att påverka vilka hanteringsverktyg som ska finnas tillgängliga för kunden via molntjänsten.

Den fjärde leveransmodellen utgörs av en hybrid mellan åtminstone två av de tre ovanstående huvudmodellerna. Hybridmodellen särskiljer sig genom att olika moln tillåter en viss överföring av data trots en separation av kundgrupperna.\textsuperscript{35}

\section*{2.3 Molntjänster och outsourcing}

\subsection*{2.3.1 Vad är outsourcing?}

Outsourcing är ett låneord från engelskan, vars kanske närmaste motsvarighet i det svenska språket är utkontraktering. Den svenska termen har dock inte förankrat sig på samma sätt i språkbruket som ordet outsourcing har gjort, varför termen outsourcing används i denna uppsats. Enligt Svenska Akademien ordböcker över svenska språket betyder outsourcing ”utläggning av verksamhet på entreprenad”. Outsourcing är sålunda, precis som molntjänster, en typ av affärsmodell för att hantera vissa verksamhetsfunktioner. Vid outsourcing överföras ansvar för en del av verksamheten på en aktör utanför den egna organisationen. Ansvaret för verksamhetsfunktionerna regleras i avtal mellan den outsourcingande parten och leverantören och under avtalets löptid svarar leverantören för kundens behov. Outsourcing som term omfattar dock inte till exempel konsultinköp eller en organisations bolagisering av en verksamhetsfunktion i sig, såväl inte bolagiseringen även innebär att en extern part tar över ägansvaret.\textsuperscript{36}

\subsection*{2.3.2 Är molntjänstavtal outsourcing?}

När IT-funktioner som innefattar personuppgiftsbehandling ska outsourcas kan detta ske antingen på traditionellt vis, så kallad IT-outsourcing [ITO]), eller genom molntjänster. I den ibland

\textsuperscript{32} NIST, s. 7 och Magnusson Sjöberg m.fl., s. 446.  
\textsuperscript{33} NIST, s. 7 och Magnusson Sjöberg m.fl., s. 446 f.  
\textsuperscript{34} NIST, s. 7 och Magnusson Sjöberg m.fl., s. 467.  
\textsuperscript{35} NIST, s. 7.  
\textsuperscript{36} Lindberg m.fl., s. 15.
forekommande diskussionen om huruvida man bör använda ”molntjänster eller outsourcing” refererar begreppet outsourcing till ITO.

Molntjänster som affärsmodell har varit revolutionerande för IT-marknaden vilket även visat sig i konkurrensen bland leverantörer av IT-resurser. Skillnaderna mellan köp av molntjänster och ITO är betydande på flera sätt. ITO föregås ofta av omfattande avtalsförhandlingar medan nyttjande av molntjänster ofta sker enligt allmänna villkor dikterade av leverantören. Förhandlingarna inför en ITO utmynnar ofta i ett flerårigt kontrakt medan molntjänstavtal kan ingås och avslutas av köparen själv vid behov. Köpbeloppet vid en ITO innebär fasta kostnader som justeras baserat på vissa förutbestämda parametrar medan molntjänster är som ”IT på kran” och kan faktureras per timme. 37

Molntjänster skiljer sig som affärsmodell kraftigt från de traditionella affärsmodellerna för IT-tjänster. Dessa skillnader har dock ingen egentlig bäring på vad som ska klassificeras som outsourcing, varför begreppet ITO kunde verka missvisande i och med att det indikerar att molntjänster inte är outsourcing. Vid ett molntjänstavtal kommer avtalsparterna överens om att leverantören ska ansvara för åtminstone delar av bland annat drift, fysisk säkerhet och underhåll av berörda datahallar. Beröende på den avtalade molntjänstens modell kan leverantören även ansvara för till exempel informationssäkerhet och programvara. När ansvaret för dessa funktioner övergår från köparen till leverantören genom ett avtal föreligger en typ av outsourcing. Molntjänster och annan typ av outsourcing särbehandlas inte juridiskt sett. I den fortsatta framställningen är därför utgångspunkten att köp av molntjänster är en form av outsourcing när köparen tidigare ansvarat för de processer och funktioner som molntjänstleverantören tillhandahåller. 38

2.4 Statistik

I detta sammanhang är det av intresse att diskutera hur ofta myndigheter använder molntjänster och i vilken utsträckning dessa används för personuppgiftsbehandling. Pensionsmyndigheten genomförde under oktober månad år 2015 en enkätundersökning i syfte att kartlägga myndigheternas användning av molntjänster. Totalt 188 svenska myndigheter mottog enkäten och 148 myndigheter svarade, vilket ger en svarsfrekvens om 79%. I nedanstående tabeller illustreras svaren på de specifika frågorna i procent med avrundning till närmaste heltal. Antalet svarande på varje fråga avviker från den generella svarsfrekvensen i enkäten, dels på grund av att myndigheterna hade möjlighet att hoppa över frågor, dels på grund av att vissa frågor ställdes som följdfrågor på jakande svar. Antalet svarande på varje fråga redovisar därför genom fotnoterna.

| Använder myndigheten idag [oktober 2015] molntjänster39? |
|---------------------------------|----------------|----------------|
| Använd | Använd inte | Vet ej om det används |
| **SaaS**40 | 78% | 21% | 1% |
| **PaaS**41 | 23% | 73% | 4% |
| **IaaS**42 | 26% | 71% | 3% |

---

37 Pensionsmyndigheten, Molntjänster i staten, s. 12.
38 Pensionsmyndigheten, Molntjänster i staten, s. 37.
39 Dessvärre beskriver inte Pensionsmyndigheten hur de definierade molntjänster i enkäten.
40 140 svarande.
41 141 svarande.
42 141 svarande.
Myndigheters nyttjande av molntjänster idag

Vilken typ av information finns i molntjänsten?

<table>
<thead>
<tr>
<th></th>
<th>Används för personuppgifter</th>
<th>Används för känsliga personuppgifter</th>
<th>Har tecknat personuppgiftsbiträdesavtal</th>
<th>Genomför alltid risk- och sårbarhetsanalys</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS</td>
<td>54%</td>
<td>9%</td>
<td>39%</td>
<td>34%</td>
</tr>
<tr>
<td>PaaS</td>
<td>45%</td>
<td>15%</td>
<td>43%</td>
<td>62%</td>
</tr>
<tr>
<td>IaaS</td>
<td>64%</td>
<td>25%</td>
<td>56%</td>
<td>57%</td>
</tr>
</tbody>
</table>

Trots att antalet svarande myndigheter i vissa fall är lågt ger statistiken en hel del intressanta upplysningar. Det synes till exempel vara vanligt att myndigheter använder sig av molntjänster i sin verksamhet. Det ska dock påpekas att enkäten inte ger svar på vem som tillhandahåller molntjänsterna. En del av molntjänsterna kan till exempel tillhandahållas av myndigheten själv eller av andra myndigheter och inte av marknadsaktörer.

Av de tjänstemodeller som används är SaaS den överlägset vanligaste modellen. Många myndigheter har dock avstängt från att närmare besvara frågan om vilken typ av information som hanteras i molntjänsterna. Detta kan bero på flera olika saker. En anledning kunde vara att många myndigheter själva inte har en tillräckligt god överblick av informationsflödet. Statistiken ger även upplysningar om att många myndigheter inte ingått personuppgiftsbiträdesavtal trots att de behandlar personuppgifter via molntjänster. Dessutom är andelen myndigheter som behandlar personuppgifter via molntjänster och som alltid gör en risk- och sårbarhetsanalys lägre än önskvärt.

2.5 SAMMANFATTNING


Molntjänster kan erbjudas i tre olika former av tjänstemodeller. Dessa tre sätt skiljer sig åt genom vilken mängd ansvar som leverantören åtar sig i molntjänstavtalet för framförallt programvaran. I fallande ordning åtar sig leverantören störst ansvar vid SaaS åtföljt av PaaS och slutligen IaaS. Molntjänster kan även erbjudas med fyra olika leveransformer. Leveransmodellerna skiljer sig åt beroende...

43 Se uppsatsens kapitel 4.1 “Vad är personuppgifter” för en beskrivning av vilken typ av information som utgör personuppgifter.
44 Se kapitel 6.3.2 ”Informationsklassificering” för en beskrivning av vilka personuppgifter som är känsliga.
45 92 svarande.
46 20-21 svarande.
47 27-28 svarande.
på molntjänsternas kundgrupper. Privata moln tillhandahålls endast en kund medan gemensamma moln tillhandahålls en grupp av kunder med liknande behov. Publika moln tillhandahålls allmänheten och hybridmoln erbjuds som variationer av de ovanstående leveransmodellerna.


3 ÖVERBLICK AV INTEGRITETSSKYDDSREGLERINGEN

Integritetsskyddet för personuppgifter i digitala miljöer är omfattande. Regelverket spänner över alla normnivåer i den nationella rätten och sträcker sig över både europeisk unionsrätt och annan internationell rätt. Utöver detta finns uttalanden av myndigheter så som allmänna råd och andra vägledande dokument. I detta avsnitt ges en orientering bland sådana rättsakter som är särskilt relevanta för att besvara uppsatsens frågeställning eller som är av betydelse för att kunna sätta de relevanta rättsreglerna i sitt sammanhang.


3.1 INTEGRITETSSKYDDSREGLERINGENS UPPDELNING I EN GENERELL OCH SPECIELL DEL

Den generella integritetsskyddsregleringen utgörs idag främst av personuppgiftslagen, den till personuppgiftslagen kompletterande personuppgiftsförordningen och de därtill hörrande allmänna föreskrifterna av Datainspektionen. Som tidigare nämnts kommer emellertid GDPR förändra det juridiska landskapet inom integritetsskyddsflagstiftningen i Sverige.

Dataskyddsdirektivet kommer upphävas i samband med att GDPR börjar tillämpas den 25 maj 2018. Dataskyddsdirektivet har huvudsakligen genomförts i svensk rätt genom personuppgiftslagen, vilken av den anledningen också kommer upphävas. Även personuppgiftsförordningen och Datainspektionsens allmänna föreskrifter, vars regler utfärdats på basis av personuppgiftslagen, kommer behöva upphävas av regeringen respektive Datainspektionen i samband med att dataskyddsförordning börjar tillämpas.48

Eftersom dataskyddsförordningen både medger och förutsätter nationell särreglering för myndigheters behandling av personuppgifter har regeringen respektive Dataskyddsutredningen föreslagit att

GDPR ska kompletteras med en ny dataskyddslag och en ny svensk dataskyddsförordning.49 Riksdagen kan förväntas ta ställning till förslagen inom kort. Regeringen har nämligen föreslagit att dataskyddslagen ska träda i kraft i samband med att GDPR börjar tillämpas.50 Den generella delen av integritetsskyddslagstiftningen kan alltså i framtiden förväntas bestå av GDPR, dataskyddslagen, den svenska dataskyddsförordningen och nya föreskrifter från Datainspektionen.

Den generella integritetslagstiftningen karaktäriseras av att den, med vissa undantag som till exempel brottsbekämpande verksamhet, är tillämplig oavsett vilken verksamhet som avses. Ingen skillnad görs mellan privat och offentlig verksamhet eller olika marknadssektorer. Den speciella integritetsskyddsregleringen däremot består av specialregler som i förhållande till den generella regleringen både utsträcker och inskränker ansvaret för olika verksamhetsområden eller specifika myndigheter. Den generella integritetsskyddsregleringen har varit och föreslås att fortsatt bli subsidiär i förhållande till den speciella integritetsskyddsregleringen. Som beskrivits ovan kommer dock GDPR:s regler på grund av principen om unionsrättens företräde ha företräde framför den speciella integritetsskyddsregleringen.51

Den speciella integritetsskyddsregleringen består av ett stort antal lagar och förordningar som i detalj reglerar hur personuppgifter får hanteras och vem som har ansvar för dem. Detta regelkomplex kallas ofta för registerförfattningarna. Även på detta område pågår en rad lagstiftningsarbeten.

År 2011 tillsatte regeringen en utredning, Informationshanteringsutredningen, i syfte att se över registerförfattningarna och skapa rättsliga förutsättningar för att kombinera en mer effektiv e-förvaltning och ett högt integritetsskydd för enskilda.52 Uppdraget expanerades senare till att utreda möjligheterna för att skapa en generell, enhetlig och i vart fall delvis samlad reglering av myndigheters personuppgiftsbehandling.53 I april år 2015 presenterade utredningen sitt slutbetänkande, vilket innehöll ett förslag om en ny myndighetsdatalag.54 Vid den tiden hade emellertid arbetet bakom GDPR kommit så pass långt att regeringen valde att avvakta tills vidare med att vidta ytterligare åtgärder. Framtiden får utvisa om de förslag som Informationsutredningen lagt för att skapa en samlad och tydlig reglering för personuppgiftsbehandling på myndighetsområdet kan få nytt liv i framtiden. Det finns även andra utredningar och förslag vilka rör den speciella integritetsskyddsregleringen. Författningssändringarna som föreslås är dock begränsade till att anpassa de svenska registerförfattningarna till bestämmelserna i GDPR.55

3.2 **Integritetsskydd och rättssystemets normativa hierarki**

Enligt den allmänna rättsprincipen om dualism ska inte internationella konventioner beaktas vid rättsstillämpningen i svenska domstolar.56 Domstolarna ska endast beakta sådana rättsregler som genomförts i den svenska rättsordningen genom transformation eller inkorporation. Transformation innebär att den svenska lagstiftaren skapar nya rättsregler som tillgodos ser konventionens krav. Inkorporation innebär och andra sidan att den svenska lagstiftaren skapar en ny lagstiftningsakt som proklamerar att konventio nens innehåll gäller som svensk lag. Den dualistiska principen mildras något av

49 Prop. 2017/18:105, s. 7 och SOU 2017:39, s. 55.
51 Se uppsatsens kapitel 3.2 ”Integritetsskydd och rättssystemets normativa hierarki” för en närmare beskrivning av principen om unionsrättens företräde.
52 Dir. 2011:86
54 SOU 2015:39.
56 För följande diskussion se Bernitz & Kjellgren, s. 77 ff.
en annan princip om konventionskonform tolkning. Denna princip innebär att svenska rättsregler ska tolkas i ljuset av de konventioner regeringen ingått. När det vid rättsstillämpningen finns utrymme för tolkning ska domstolen sålunda välja ett tolkningsalternativ som innebär att konventionens krav uppfylls.

Vad avser rättsakter från den Europeiska unionen är saken emellertid en annan, trots att även den europeiska unionsrätten i grunden bygger på internationella konventioner i form av Fördraget om Europeiska unionen [FEU], Fördraget om Europeiska unionens funktionssätt [FEUF] och Europeiska unionens stadga om de grundläggande rättigheterna [rättighetsstadgan]. Den Europeiska unionens domstol och Europaparlamentet, till vilket ledamöter väljs direkt av Europas folk, ger unionen en annan demokratisk förankring som legitimerar en överstatlig dimension av den europeiska unionsrätten. Den Europeiska unionens domstol har funnit att den europeiska unionsrätten, på grund av sin särskilda karaktär, har ett företräde framför nationell lagstiftning inom unionsrättens gränser.


Allmänna råd och andra vägledande dokument från svenska myndigheter och myndigheter inom ramen för den Europeiska unionen är skapade av de anställda hos respektive myndighet. Dessa dokument har därför ingen demokratisk förankring och tillskrivs därför ingen bindande kraft. Ibland har dessa uttalanden trots det ett stort värde när de uppfyller ett regleringsbehov. I dessa situationer får uttalandena, trots att de inte har en teoretisk bindande kraft, ändå en normerande kraft de facto.

Inte heller förslag till nya lagar har någon normerande kraft. Sådana förslag har ju inte (ännu) bifallits av den folvalda riksdagen och vunnit demokratisk legitimitet. När lagstiftaren signalerar att den har för avsikt att genomföra ny lagstiftning på ett visst område kan det dock vara av intresse för marknaden att följa utvecklingen. Är sannolikheten stor för att ett visst lagstiftningsförslag kommer beslutas kan aktörerna på marknaden nämligen börja inrätta sig efter förslaget redan innan det börjar tillämpas för att minimera övergångseffekterna. Av den anledningen kan även lagförslag sägas ha en praktiskt normerande effekt i någon utsträckning.

3.3 INTERNATIONELLA ÅTAGANDEN AVSEENDE INTEGRITETSSKYDD

På det internationella planet har rätten till personlig integritet fastslagits som en mänsklig rättighet av världssamfundet genom art. 12 i Förenta nationernas generalförsamlings allmänna förklaring om de mänskliga rättigheterna av den 10 december 1948. Personlig integritet har även fastslagits som en rätt för alla europeiska invånare genom den av Sverige år 1952 ratificerade Europeiska konventionen

57 Då Europeiska gemenskapernas domstol.
58 Mål 6/64/EG Costa mot ENEL, REG 1964, s. 585, v. 1, på s. 218. För en redogörelse av den efterföljande rättsutvecklingen, se Bernitz & Kjellgren s. 77 ff.
59 Se Fördraget om Europeiska unionens funktionssätt [cit. FEUF] art. 288(1) ang. vilka rättsakter som finns i unionen.
60 FEUF art. 291(1).
61 Bernitz & Kjellgren, s. 31 och FEUF, art 288(2).
62 Bernitz & Kjellgren, s. 31 f.

Artikel 8 i EKMR innebär att en konventionsstat bara kan göra intrång i enskildas personliga integritet om det uppfyller tre krav. För det första ska det ske genom lagstöd, för det andra ska det ske för ett i bestämmelsen legitimt ändamål och för det tredje ska det vara nödvändigt i ett demokratiskt samhälle. Dessa krav har utvecklats i Europadomstolens praxis. Domstolen har förklarat att kravet på lagstöd även innefattar ett kvalitetskrav på lagen i fråga. Lagregeln ska vara förutsebar, tillgänglig och förenlig med rättsstatliga principer.[^64] Domstolen har även förklarat att kravet på att intrånget ska vara godtagbart i ett demokratiskt samhälle ska tolkas som angelägna samhälleliga behov och innebär ett krav på proportionalitet och att skälen är relevanta och tillräckliga.[^65]


### 3.4 INTEGRITETSSKYDD INOM DEN EUROPEISKA UNIONENS PRIMÄRRÄTT


[^63]: SÖ 1952:35.
[^64]: Magnusson Sjöberg m.fl., s. 169.
[^65]: Magnusson Sjöberg m.fl., s. 170.
[^66]: SÖ 1982:50.
[^67]: FEU, art. 6(3).
Integritetsskyddet i den rättighetsstadgan återfinns under artiklarna 7 och 51(1) och motsvarar i allt väsentligt de krav som upptäcks på integritetsskyddsslagstiftningen i EKMR. Rättighetsstadgan medger ett längre gående skydd än vad som ges i EKMR men medför aldrig några inskränkningar i det skydden. Tillämpningen av EKMR som allmän princip i unionsrätten skiljer sig också åt på det viset att den bara aktualliseras i svenska domstolar vid tillämpning av unionsrätt.

3.5 **Integritetsskydd i grundlagen**

I Sveriges grundlag finns skyddet för den personliga integriteten i regeringsformens kapitel om de grundläggande fri- och rättigheterna. I 2 kap. 6 § 1 st. RF framgår bland annat att ”[v]ar och en är --- skyddad mot kroppvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtryckt försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande.” I andra stycket framgår att ”var och en gentemot det allmänna [är] skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.”

Varje begränsning från detta skydd får enligt 2 kap. 20 § 1 st. p. 2 RF bara ske genom lag. Enligt 2 kap. 21 § RF får en sådan begränsning i lagen bara ske för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle och aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamålet. Det finns ingen skillnad i skyddet mellan svenska och utländska medborgare enligt kap. 2 § 25 RF.

Enskilda åtnjuter endast ett skydd för den personliga integriteten gentemot det allmänna genom denna reglering. Regeln ger inget skydd för enskilda mot andra privata subjekt. Regleringen omfattar endast ”betydande ingrepp”, vilket i förarbetena beskrivs som sådana ingrepp som är särskilt känsliga med beaktande av ingreppets art, omfattning och ändamål samt andra omständigheter som kan ha betydelse vid bedömningen.

Inskränkningar i den personliga integriteten får bara ske på ett visst sätt, nämligen genom lag. Regleringen i grundlagen innebär ett krav gentemot lagstiftaren själv att en lag om allmänt skydd för enskildas personliga integritet gentemot det allmänna måste finnas i lag. Eftersom begränsningarna av betydande intrång i den personliga integriteten måste ske genom lag krävs lagstöd för varje sådant intrång som utförs av myndigheter.

Varje begränsning från detta skydd får enligt 2 kap. 20 § 1 st. p. 2 RF bara ske genom lag. Enligt 2 kap. 21 § RF får en sådan begränsning i lagen bara ske för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle och aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamålet. Det finns ingen skillnad i skyddet mellan svenska och utländska medborgare enligt kap. 2 § 25 RF.

Enskilda åtnjuter endast ett skydd för den personliga integriteten gentemot det allmänna genom denna reglering. Regeln ger inget skydd för enskilda mot andra privata subjekt. Regleringen omfattar endast ”betydande ingrepp”, vilket i förarbetena beskrivs som sådana ingrepp som är särskilt känsliga med beaktande av ingreppets art, omfattning och ändamål samt andra omständigheter som kan ha betydelse vid bedömningen.

Inskränkningar i den personliga integriteten får bara ske på ett visst sätt, nämligen genom lag. Regleringen i grundlagen innebär ett krav gentemot lagstiftaren själv att en lag om allmänt skydd för enskildas personliga integritet gentemot det allmänna måste finnas i lag. Eftersom begränsningarna av betydande intrång i den personliga integriteten måste ske genom lag krävs lagstöd för varje sådant intrång som utförs av myndigheter.

I grundlagen ges ingen legaldefinition av vad personlig integritet är. Förarbetena till lagen beskriver istället att någon sådan definition inte var nödvändig för att bedöma vilka intressen som bör omfattas av skyddet. Någon definition av vad som avses med personlig integritet står inte heller att finna i någon annan del av normsystemet. Ofta beskrivs den personliga integriteten som en enskilds personliga sfär eller en rätt för enskilda att bli lämnade i fred.

3.6 **Den allmänna dataiskyddsförordningen (GDPR)**

unionen. GDPR lämnar utrymme för kompletterande nationella bestämmelser i vissa delar och förutsätter nationella bestämmelser i andra. Delar av förordningen kan dessutom genomföras i nationell rätt genom förtydliganden eller begränsningar i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga.\(^73\) Detta har beskrivits som att förordningen har en direktivliknande karaktär.\(^74\)

Dataskyddsförordningen syftar till att säkerställa det fria flödet av personuppgifter inom unionen genom att undanröja skillnader i medlemsstaternas integritetsskyddslagstiftningar.\(^75\) Skyddet ska harmoniseras för att konkurrensen mellan den ekonomiska verksamhet som bedrivs över landsgränserna inom unionen inte ska snedvridas.\(^76\) Förordningen manifesterar därmed en strävan att upprätthålla en likhet i förutsättningarna för aktörerna på den inre marknaden.

Ett annat rättspolitiskt syfte bakom förordningen är att den snabba teknologiska utvecklingen medför ett ökat skyddsbehov. Teknologin har drivit på insamlingen och delningen av personuppgifter och orsakat ett behov av en högre skyddsnivå. Det alltmer globaliserade sociala och ekonomiska livet medför nämligen att enskilda uppgifter sprids i betydligt större omfattning.

Av art. 2(2) i GDPR framgår att förordningen inte är tillämplig på sådan personuppgiftsbehandling som sker i fyra särskilt angivna situationer. Dessa situationer är (1) verksamhet utanför unionsrättens gränser (2) verksamhet inom Europeiska unionens gemensamma utrikes- och säkerhetspolitik (3) personuppgiftsbehandling för privat bruk och (4) brottsförebyggande verksamhet. Huruvida ett område ligger inom unionsrättens gränser tolkas genom en granskning av den Europeiska unionens kompetensområden. Vilka områden som tillkommer den Europeiska unionens respektive medlemsstaternas kompetens framgår av art. 3-6 i FEU. Vilken politik som ingår i den Europeiska unionens gemensamma utrikes- och säkerhetspolitik framgår av avd. 5 kap. 2 FEU.


De två återstående undantagen om personuppgiftsbehandling för privat bruk och för brottsförebyggande verksamhet saknar intresse vid en behandling av uppsatsens frågeställning eftersom ingen personuppgiftsbehandling för privat bruk kan ske inom myndigheters verksamhet och eftersom brottsförebyggande verksamhet undantagits från uppsatsens behandlingsområde.

Av art. 3(1) i GDPR framgår att regleringen gäller så snart antingen ett personuppgiftsbiträde eller en personuppgiftsansvarig är etablerad i unionen. Även om de flesta svenska myndigheter naturligtvis är etablerade inom unionen kan läget vara annorlunda för till exempel diplomatiska beskickningar och

\(^73\) GDPR, beaktandeskäl 8.
\(^74\) SOU 2017:39 s. 72.
\(^75\) GDPR, art 1.
\(^76\) GDPR, beaktandeskäl 9.
\(^77\) Prop. 2017/18:105, s. 7 i förslaget till lagtext, 2 kap. 1 §.
konsulat. Även personuppgiftsbehandling under dessa förhållanden omfattas dock av förordningen om den personuppgiftsansvarige är etablerade på en plats där svensk rätt gäller enligt folkrätten enligt art. 3(3).78 Det geografiska tillämpningsområdet medför sålunda få begränsningar gällande tillämpningsområdet av GDPR för svenska myndigheter.

3.7 ÖFFTENLIGHEETS- OCH SEKRETESSLAGEN

I OSL finns sekretessregler till skydd för många olika intressen. Många sekretessregler är till skydd för uppgifter om enskildas personliga och ekonomiska förhållanden. Dessa regler syftar till att säkerställa enskildas rätt till en privat sfär och är en del av den svenska integritetsskyddsregleringen.

OSL är en omfattande lag som består av 44 kapitel uppdelade i sju olika avdelningar. De bestämmelser som är till skydd för enskildas privata sfär regleras främst i den femte avdelningen, detta vill säga kapitel 21 till kapitel 40. Vilka personuppgifter som är sekretessreglerade regleras främst i dessa kapitel.

Alla svenska myndigheter och personer som fått kännedom om sekretessreglerade uppgifter genom att delta i myndigheters verksamheter omfattas av sekretessen enligt 2 kap 1 § OSL. Med deltagande i myndigheters verksamhet avses anställning, uppdrag, tjänsteplikt eller andra liknande grunder. Enligt 8 kap 1-2 §§ OSL gäller sekretessen gentemot andra myndigheter, andra självständiga verksamhetsgrenar inom den egna myndigheten och gentemot enskilda. OSL är inte subsidiär i förhållande till annan lagstiftning. När en uppgift är sekretessreglerad enligt bestämmelserna i OSL får myndigheter inte lämna ut uppgiften såvida inte annat anges i OSL eller i en lag eller förordning som OSL hävvisar till, 7 kap 1 och 3 §§ samt 8 kap 1 § OSL.

3.8 FÖRSLAGET TILL NY DATASKYDDSLAG OCH NY SVENSK DATASKYDDSFRÖORDNING


Ändamålen bakom dataskyddslagen och den svenska dataskyddsförordningen är inte att inskränka eller utvidga möjligheterna för personuppgiftsbehandling mer än vad som redan sker genom den allmänna dataskyddslagen. Istället är syftet att de i den allmänna dataskyddsordningen stipulerade bestämmelserna ska förtydligas.

Både dataskyddslagen och den svenska dataskyddsförordningen föreslås vara generella på så vis att de inte enbart innehåller bestämmelser som är specifika för vissa myndigheter på det sätt som registerförfattningarna gör. Bestämmelserna gäller istället generellt för både privat och offentlig sektor precis som GDPR.79

Bestämmelserna föreslås bli subsidiära i förhållande till andra lagar och förordningar.80 Detta innebär att registerförfattningarna ska tillämpas istället för bestämmelserna i dataskyddslagen och den svenska dataskyddsförordningen när en regelkonflikt föreligger.

78 GDPR, beaktandeskäl 25.
79 SOU 2017:39, s. 39, i förslaget till lagtext, 1 kap. 2 §.
80 SOU 2017:39, s. 39, i förslaget till lagtext, 3 §.
Dataskyddslagen utvidgar tillämpningsområdet för GDPR till att gälla även sådana rättsområden som inte omfattas av unionsrätten.81

3.9 SAMMANFATTNING


Den speciella integritetsskyddssommen består av hundratals lagar som i detalj reglerar personuppgiftsbehandling i specifika verksamheter och myndigheter. Flera statliga utredningar pågår för att anpassa registerförfattningarna till GDPR. Informationshanteringsutredningen lade år 2015 fram ett förslag som skulle leda till en mer samlad reglering av registerförfattningarna men detta förslag har ännu inte lett till några åtgärder från lagstiftarens sida.

Det finns ingen allmänt accepterad definition av personlig integritet trots att den fastslagits som en grundläggande mänsklig rättighet i flera internationella konventioner, däribland EKMR. Begreppets innebördd kan dock uttolkas indirekt genom bland annat Europadomstolens praxis. EKMR binder konventionsstaterna så att inskränkningar i den personliga integriteten bara kan göras under vissa förutsättningar. EKMR har getts en hög status i svensk rätt eftersom ett stadgande i grundlagen fastslår

81 SOU 2017:39, s. 39, i förslaget till lagtext, 2 §.
att nya lagar inte får stiftas om de är stridiga med konventionen. EKMR har dessutom lyfts upp som allmän princip och gjorts till en del av den Europeiska unionens primärrätt. I de fall unionsrätten aktualiseras har därför EKMR förerträde framför annan lag i Sverige. Inom Europeiska unionen tillförsakras alla invånare i unionen dessutom respekt för den personliga integriteten genom både rättighetsstadgan och FEUF. I allt väsentligt ser skyddet för den personliga integriteten inom unionens primärrätt ut på samma sätt som i EKMR.

I den svenska grundlagens rättighetskaptel skyddas alla svenska medborgare och utlänningar mot statliga ingrepp som innebär betydande intrång i den personliga integriteten. Begreppen av grundlagsskyddet får bara ske under vissa förutsättningar.

4 PERSONUPPGIFTER OCH MYNDIGHETERS ANSVAR

För att läsaren ska veta under vilka förhållanden som framställningens analys och slutsatser är applicerbara är det viktigt att tillämpningsområdet av rättsreglerna som utreds preciseras. I detta kapitel utreds den närmare innebörden av termerna personuppgifter, personuppgiftsbehandling och personuppgiftsansvar. Som framgår nedan är dessa begrepp centrala för tillämpningen av integritets skyddslagstiftningen och för att uppsatsens analys och slutsatser ska vara applucerbara. I utredningen ställs begreppen i förhållande till myndigheter och molntjänster.

Av art. 2(1) i GDPR framgår att förordningen ska tillämpas vid ”sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register”. De uppgifter som omfattas av regleringen avgörs sålunda genom en utredning i två olika steg: (1) Är det en personuppgift? (2) Ingår uppgifterna i en automatisk behandling eller i ett register?

4.1 VAD BETYDER PERSONUPPGIFTER?

Definitionen av personuppgifter är central både för tillämpningsområdet av GDPR och registerförfattningarna. Det juridiska begreppet ”personuppgift” innefattar ett större spektrum av uppgifter än vad som avses med begreppet i vardagligt tal. Begreppet begränsas inte till exempelvis namn och personnummer utan omfattar alla typer av uppgifter som kan användas för att identifiera en enskild person.

Dataskyddsdirektivet innehåller en förordningsautonom definition av begreppet i art. 4(1) som anger att personuppgifter är ”varje upplysning som avser en identifierad eller identifierbar fysisk person”. Både direkt och indirekt identifiering innefattas i begreppet. I artikeln exemplifieras detta genom en förklaring om att namn, identifikationsnummer, lokaliseringuppgifter, online-identifikator eller andra typer av identifierande utgör personuppgifter. För att markera att tolkningen av personuppgifter ska ske brett understryks också att andra ”faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet” kan vara personuppgifter.

I 3 § personuppgiftslagen finns en svensk legaldefinition av begreppet. Paragrafen anger att personuppgifter är ”[a]ll slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.” Legaldefinitionen är en implementering av dataskyddsdirektivets definition av personuppgifter i art. 2(a). Dataskyddsdirektivets definition är i princip identisk med definitionen i GDPR. Detta

---

82 SOU 1997:39, s. 95 f.
83 GDPR exemplifierar med lokaliseringsuppgifter och online-identifikatorer (GDPR, beaktandeskäl 30) samt att faktorer som är specifika för en persons genetiska identitet (se GDPR beaktande 34) utgör personuppgifter. Se även dataskyddsutredningens bedömning SOU 2017:39, s. 270.
innebär att man vid tolkningen av innebörden av begreppet personuppgifter i GDPR med viss försiktighet kan använda sig av den begreppstolkning som gjorts på basis av dataskyddsdirektivets bestämmelse.

För att uppnå större likhet vid rättstillämpningen bland medlemsstaterna har WP29 detaljerat förklarat hur begreppet personuppgifter i dataskyddsdirektivet ska tolkas genom ett uttalande. För att uppnå större likhet vid rättstillämpningen bland medlemsstaterna har WP29 detaljerat förklarat hur begreppet personuppgifter i dataskyddsdirektivet ska tolkas genom ett uttalande.

4.1.1 Personuppgifters fyra beståndsdelar

Begreppet personuppgifter ska förstås mycket brett men har inte en obegränsad räckvidd. GDPRs definition av personuppgifter kan delas upp i fyra olika beståndsdelar, nämligen (1) varje upplysning (2) som avser en (3) identifierad eller identifierbar (4) fysisk person. Bara när samtliga beståndsdelar föreligger är det fråga om en personuppgift. De fyra förutsättningarna är alltså kumulativa.

4.1.2 Beståndsdelens "varje upplysning"


4.1.3 Beståndsdelens "som avser en"

4.1.4 Beståndsdelens “identifierad eller identifierbar”


Enligt GDPR art. 4.5. är pseudonymiserade uppgifter sådan information som inte kan tillskrivas en person utan separat kompletterande information.\(^9^1\) Personuppgifter som blivit pseudonymiserade är dock alltjämt personuppgifter, så länge den kompletterande informationen med vilken en person kan identifieras existerar. Uppgifter som anonymiserats och inte längre hänför sig till en identifierbar person är inte personuppgifter.

4.1.5 Beståndsdelens “fysisk person”

Med fysisk person avses alla människor, oavsett medborgarskap eller hemvist. Juridiska personer omfattas inte.\(^9^2\) De kan dock komma att skyddas indirekt om deras uppgifter kan anknytats till en fysisk person genom till exempel namnläggning eller där informationens syfte, innehåll eller resultat medför att informationen avser en fysisk person. Med fysiska personer avses levande människor varför avlidna personer inte omfattas.\(^9^3\) Inte heller ofödda människor, det vill säga foster, omfattas.\(^9^4\)

4.1.6 Ett juridiskt verktyg vid bedömningen


---

\(^8^8\) GDPR, beaktandeskäl 26.
\(^8^9\) Ang. den fortsatta diskussionen, se WP29, Personuppgiftsbegreppet, s. 12 ff.
\(^9^0\) GDPR, beaktandeskäl 30.
\(^9^1\) Ang. detta stycke, se GDPR, beaktandeskäl 26.
\(^9^2\) GDPR, beaktandeskäl 14.
\(^9^3\) GDPR, beaktandeskäl 27.
\(^9^4\) Sjöberg, Personuppgiftslag 3 § Lexino och WP29 4/2007 s. 22.

4.2 VAD BETYDER PERSONUPPGIFTSBEHANDLING?
Med behandling av personuppgifter avses alla åtgärder som vidtas beträffande personuppgifter. Be-
greppet urskiljer inga typer av hanteringsformer utan omfattar dem alla. Så snart uppgifterna hante-
ras så är det att se som en behandling i juridisk mening. Dataflycksförordningen uttrycker detta som att ”en åtgärd eller kombination av åtgärder beträffande uppgifter eller uppsättningar av per-
sonuppgifter oberoende av om de utförs automatiserat eller ej” är behandling enligt art. 4(2) i GDPR. Där exemplifieras även med en lång, icke uttömmande lista på åtgärder som omfattas: ”insamling, registrering, organiserad, strukturering, lagring, bearbetning eller ändring, framtagnings, läsning, an-
vändning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller
sammanförra, begränsning, radering eller förstöring.” Bestämmelsen kommer inte medföra någon förändring av rättsläget i samband med att den börjar tillämpas eftersom den, utöver att ett par exempel adderats, överensstämmer med de nu gällande bestämmelserna i 3 § personuppgiftslagen och art. 2(b) dataskyddsdirektivet.

Distinktionen mellan vad som utgör automatiserade behandlingar och vad som utgör manuella be-
thandlingar har betydelse för tillämpligheten av den generella integritetsskyddsreglerna på det sättet att automatiska behandlingar alltid omfattas medan manuella bara omfattas om det är fråga
om registerförring. I IT-sammanhang är en behandling dock alltid att se som automatiserad. Molt-
tjänster är ett digitalt fenomen och varför det av naturliga skäl inte kan uppstå en situation där det är fråga om manuell behandling, varför det i detta arbete saknas anledning att närmare gå in på den ju-
ridiska definitionen av register.97

4.3 VAD BETYDER PERSONUPPGIFTSANSVAR?
I art. 24 i den allmänna dataskyddsförordningen står det att den personuppgiftsansvarige ska ”genom-
föra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behand-
lingen utförs i enlighet med denna förordning.” Den som innehar personuppgiftsansvaret ansvarar sålunda för att integritetsskyddsreglerna efterlevs, även om det inte är den personuppgiftsansvarige själv som utför själva behandlingen. De regler som ska åtföljas i GDPR är många och inkluderar bland annat att uppgifterna behandlas lagligt, korrekt och öppet med integritet och konfidentialitet och att behandlingen präglas av ändamålsbegränsning, uppgiftsminimering och lagringsminimering, att infor-
mation tillhandahålls eller kommunikeras till de registrerade när så krävs, att uppgifterna raderas
eller rättas vid en berättigad begäran, att de behandlas med en lämplig säkerhetsnivå, att konse-
kvemsbedömningar upprättas och att säkerhetsincidenter anmäls. Var och en av dessa skyldigheter innebär att de personuppgiftsansvariga myndigheterna måste vidta vissa konkreta åtgärder för att möta de legala kraven. Inom ramen för det här arbetet saknas det emellertid anledning att gå in när-
mare på hur man avgör vilka dessa konkreta åtgärder är.

Att myndigheter ingår molntjänstavtal med molntjänstleverantörer förändrar inte myndigheternas
status som personuppgiftsansvariga. Personuppgiftsansvaret fortsätter alltid att gälla till dess

96 SOU 1997:39, s. 334.
97 Sjöberg, Lexino, 3 §, under rubriken 2.1 behandling (av personuppgifter).
förutsättningarna för bestämmandet av personuppgiftsansvar inte längre är för handen. Molntjänst-leverantörer blir emellertid personuppgiftsbiträde i förhållande till de personuppgiftsansvariga myndigheterna enligt art. 4(8) i GDPR.

4.4 **Hur kan myndigheter underkastas personuppgiftsansvar?**

Så snart det förekommer en personuppgiftsbehandling inträder ett ansvar hos någon för den behandlingen. Begreppet personuppgiftsansvarig ska tolkas förordningsautonomt enligt art. 4(7) i GDPR. Där står att personuppgiftsansvarig är ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter”. Denna reglering är identisk med tidigare bestämmelser varför ledning vid tillämpningen kan tas från den begreppstolkning som skett på basis av de tidigare bestämmelserna.98

Myndigheters personuppgiftsansvar kan uppkomma på olika sätt. Ansvaret kan uppstå ur de allmänna principerna för fastställande av personuppgiftsansvar som framgår av art. 4(7) i GDPR, nämligen om myndigheterna faktiskt bestämmer över den aktuella personuppgiftsbehandlingens ändamål och medlen. I många fall har dock ändamålet och medlen för personuppgiftsbehandlingen bestämts av lagstiftaren och inte myndigheterna. I dessa situationer kan ansvaret inträda genom att myndigheterna antingen utpekas som personuppgiftsansvariga direkt i lag eller förordning (registerförfattningarna) för en viss typ av personuppgiftsbehandling. När myndigheter utpekas som personuppgiftsansvariga i en registerförfattning behövs ingen närmare utredning av ansvaret utan det fastställs genom den aktuella bestämelsen. Slutligen kan personuppgiftsansvar uppstå för myndigheter genom att personuppgiftsbehandlingen följer som ett led i myndigheternas fullgörande av sitt uppdrag eller skyldigheter.99

4.4.1 **Registerförfattningarna**

Det finns hundratals registerförfattningar som i olika grad både inskränker och utvidgar myndigheternas ansvar för personuppgifter.100 Många registerförfattningar reglerar direkt vem som är personuppgiftsansvarig för en viss personuppgiftsbehandling.101 Förekomsten av sådana utpekanden av personuppgiftsansvar beror dock i dagsläget på vilken myndighet och vilken situation som avses. I 1 kap. 7 § i förslaget till ny myndighetsdatalag föreslås att en huvudregel införs om att ”[e]n myndighet är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.” Förslagets 4 § innehåller dock en bestämmelse som skulle göra myndighetsdatalagen subsidiär i förhållande till registerförfattningarna varför detta inte skulle innebära en utsträckning av myndigheternas personuppgiftsansvar i de delar det begränsats i registerförfattningarna.102

Registerförfattningarna reglerar sålunda ofta myndigheternas ansvar i specifika situationer. Med anledning av att den här uppsatsen behandlar generella regler för myndigheterna görs ingen närmare utredning med anledning av registerförfattningarna.

---

98 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 [cit. dataskyddsdirektivet] art. 2(2) och Personuppgiftsslagen 3 § [cit. PuL].
99 WP29, Yttrande 1/2010 om begreppen registeransvarig och registerförare, s. 10 under rubriken ”2) Registeransvar som bygger på underförstådd behörighet” [cit. WP29, yttrande 1/2010].
100 Sjöberg, Lexino, 2 §, under rubriken 2.1. ”Särskild registerlagstiftning”.
101 Törngren, David, Personuppgiftsslag (1998:204), Karnov, 1 juli 2017, 3 § under rubriken ”Personuppgiftsansvar”.
102 SOU 2015:39, s. 38.
4.4.2 Personuppgiftsansvarets tre beståndsdelar
Identifieringen av den personuppgiftsansvarige kan brytas ned i tre huvuddelar, där den första utgörs av en personlig aspekt som i förordningen formuleras som (1) ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ”. Den andra delen utgörs av möjligheten att bestämma flera personuppgiftsansvariga genom beskrivningen (2) ”som ensamt eller tillsammans med andra”. Den tredje och sista delen av begreppet definierar vilka faktorer som identifierar den personuppgiftsansvarige i orden (3) ”bestämmer ändamålen och medlen för behandlingen av personuppgifter”.

4.4.3 Beståndsdelen ”bestämmer ändamålen och medlen”

Vad som utgör ändamål och medel kan sägas motsvara frågorna varför personuppgiftsbehandlingen utfors och hur den utförs. Beslut rörande ändamålen och medlen för personuppgiftsbehandlingen medför i princip alltid ett personuppgiftsansvar. Vilken vikt som ska läggas vid medel beror dock på i vilket sammanhang personuppgiftsbehandlingen utförs. Den personuppgiftsansvarige kan till exempel anlita ett personuppgiftsbiträde, det vill säga en aktör som utför själva personuppgiftsbehandlingen på uppdrag av den personuppgiftsansvarige utan att axla personuppgiftsansvaret, art. 4.8 i det allmänna dataskyddsdirektivet. Personuppgiftsbiträden kan i vissa situationer arbeta med ett stort manöveringsutrymme utan att det generellt ges några riktlinjer. Vissa av besluten rörande medlen, både tekniska och organisatoriska, kan i dessa situationer delegeras till ett personuppgiftsbiträde utan att de innehar ett personuppgiftsansvar. Även detta avser vilka uppgifter som ska behandlas, vilka som ska få tillgång till uppgifterna och när uppgifterna ska raderas är emellertid så viktiga element i medlen att beslut i dessa frågor framkallar ett personuppgiftsansvar.

4.4.4 Beståndsdelen ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ”
Den personliga delen av begreppet innebär att den första hand är myndigheter i sig som bör betraktas som personuppgiftsansvariga för den personuppgiftsbehandling som sker inom ramen för deras verksamhet. Myndigheters separata organ kan aldrig vara personuppgiftsansvariga eftersom de saknar rättskapacitet. Fysiska personer kan dock vara personuppgiftsansvariga om det finns tydliga...

---

103 Ang. detta avsnitt, se WP29, Yttrande 1/2010 s. 8 ff.
104 Ang. detta stycke se WP29, Yttrande 1/2010 s. 12 ff.
105 Ang. detta stycke, se WP29, yttrande 1/2010 s. 15 ff.
106 Ang. denna mening, se Öman, Sören, Lindblom, Hans-Olof, Personuppgiftslagen, En kommentar, uppl. 4 med tillägg och ändringar per v. september 2017, Norstedts Juridik AB, Stockholm, den 16 februari 2018, 3 § [cit.}
omständigheter som motiverar det. När fysiska personer använder myndigheters personuppgifter för egna ändamål vilka ligger utanför ramen för myndigheternas verksamhet och deras kontrollmöjligheter kan personuppgiftsansvar inträda för den fysiska personen. Även i dessa situationer har dock myndigheter ansvar för deras säkerhetsnivå rörande den egna behandlingen.

4.4.5 Beståndsdelens ”som ensamt eller tillsammans med andra”
Möjligheterna till flera personuppgiftsansvariga inträder då flera aktörer samspelar i behandlingen. De olika aktörernas åtgärder behöver inte vara samtidiga för att de ska ses som gemensamt personuppgiftsansvariga. Åtgärderna kan istället ske under olika händelseförlopp, på olika tekniska nivåer, i etapper eller till olika grad. Bedömningen av om en aktör är gemensamt personuppgiftsansvarig görs utifrån samma kriterier som övriga bedömningar av personuppgiftsansvaret. Det avgörande är sålunda om ändamålet och de väsentliga elementen i medlen bestäms av aktörerna gemensamt.

Ett fullständigt gemensamt personuppgiftsansvar inträder om parterna gemensamt bestämmer samtliga delar av ändamålen och medlen. Deltagandet i bestämningen av dessa måste dock inte vara likadelt utan det räcker att deltagandet avsver delar av ändamålen eller delar av de väsentliga elementen i medlen. Olika grader av delaktighet i bestämmandet bör ha motsvarighet i de rättsliga konsekvenser som personuppgiftsansvaret medför. När personuppgiftsansvaret har en asymmetrisk fördelning och olika aktörer sålunda svarar endast för vissa delar av ändamålet eller medlen kan det vara en kompllicerad sak att avgöra befogenheter, rättigheter och skyldigheter. Att en aktör inte direkt kan uppfylla sina skyldigheter utesluter dock inte att denne kan ha det yttersta ansvaret för skyldigheternas fullgörande som personuppgiftsansvarig.

Gemensamt personuppgiftsansvariga har en viss flexibilitet att sinsemellan avtala om skyldigheter och ansvar så länge en fullständig reglelefterlevnad garanteras. Om avtal inte återspeglas i verkligheten kommer den rättsliga bedömningen att alltid avgöras utifrån de faktiska omständigheterna vid fastställande av ansvaret. Om fördelningen av skyldigheterna mellan de gemensamt personuppgiftsansvariga orsakar en sådan komplexitet att de registrerades rättigheter försämrar kan detta leda till att behandlingen blir otillåten. En fördelning av personuppgiftsansvaret syftar nämligen till att undanröja osäkerhet för personuppgiftsansvaret. Har parterna kommit överens om en annan tydlig och effektiv ansvarsfördelning bör den beaktas vid bestämmande av ansvaret i första hand.

Datautbyte mellan två personuppgiftsansvariga som varken delar ändamål eller medel gör dem inte gemensamt personuppgiftsansvariga. Om olika aktörer har separata ändamål och medel vad avser respektive personuppgiftsbehandling kan de ändå vara att anse som gemensamt personuppgiftsansvariga om åtgärderna på makronivå bör betraktas som en serie åtgärder med gemensamt fastställda ändamål eller medel.

4.5 SAMMANFAFTNING
Definitionen av begreppet personuppgifter ändras inte i och med GDPR. Varje upplysning som avser en identifierad eller identifierbar fysisk person är en personuppgift. Begreppet är därför omfattande och sträcker sig långt utöver vad man i vardagligt tal menar när man använder ordet personuppgifter. Ingen skillnad i bedömningen av vad som utgör personuppgifter görs beroende av en uppgifts natur, innehåll eller format. Upplysningens innehåll, syfte eller resultat måste dock anknyta till en fysisk person för att det ska vara fråga om en personuppgift.


107 Ang. detta stycke, se WP29, Yttrande 1/2010 s. 17 ff.

Behandling är ett brett uttryck som omfattar alla åtgärder som vidtas beträffande personuppgifter. Personuppgiftsbehandling medför sålunda ingen begränsning i fråga om vilka åtgärder en personuppgiftsbehandling består av. I IT-sammanhang är alla behandlingar automatiserade behandlingar, varför det inte är av relevans huruvida uppgifterna ingår eller ska ingå i register.


När en registerförfattning utpekar myndigheter som personuppgiftsansvariga för en viss personuppgiftsbehandling behövs ingen vidare utredning av frågan. Personuppgiftsansvaret fastställs då direkt utifrån den aktuella författningsbestämmelsen. Huruvida myndigheter är personuppgiftsansvariga utifrån de allmänna principerna måste avgöras genom en bedömning i tre olika led.


5  ALLMÄNT OM LAGLIGHETSPRÖVNINGEN

5.1 LAGLIGHETSPRÖVNING OCH LÄMPLIGHETSPRÖVNING

Den svenska offentliga förvaltningens självständighet är ett av Sveriges konstitutionella särdrag. Självständigheten har gamla anor och härstammar från Sveriges tid som stormakt, då riket var så stort att myndigheterna inte ansågs kunna styras tillräckligt effektivt från Stockholm. De svenska förvaltningsmyndigheternas starka ställning innebär att de har stor frihet att själva avgöra hur de ska arbeta för att fullgöra sina upphand.\textsuperscript{108} Detta innebär bland annat att de efter eget skön har möjlighet att avgöra hur de ska lägga upp delar av sin verksamhet. En myndighet kan till exempel välja att dra alla delar av sin verksamhet i egen regi eller att outsourcing vissa delar av den, låt vara att möjligheterna begränsas bland annat av att den endast får ske med stöd av lag i de fall den innefattar myndighetsutövning.\textsuperscript{109}


Hur förvaltningsmyndigheter bör resonerar i sina egna lämplighetsbedömningar av huruvida den bör använda affärsmodellen molntjänster för behandling av personuppgifter faller utanför uppsatsens syfte. När det i den fortsatta framställningen talas om lämplighetsprövningar avses därför sådana som ryms inom ramen för laglighetsprövningen.

5.2 KLARLÄGGANDE AV OMSTÅNDIGHETER

En laglighetsprövning börjar med att klarlägga vilka omständigheter som föreligger i den specifika situationen. Dessa omständigheter är nämligen av vikt för att man ska kunna ta reda på vilka krav som ställs och vilka regelverk som blir tillämpliga. För att kunna genomföra en analys av lagligheten inför en planerad upphandling av molntjänster för personuppgiftshantering måste myndigheterna bland annat veta vilken typ av information som kommer hanteras, vem som kommer hantera.

\textsuperscript{108} 12 kap. 2-3 §§ RF.
\textsuperscript{109} 12 kap. 4 § RF.
informationen, hur informationen kommer hanteras och var informationen kommer hanteras rent geografiskt.

Molntjänstleverantörer har sällan tillräckligt bra transparens i sina verksamheter för att dessa frågor ska gå att informera sig om enbart genom en studie av standardavtalen eller genom öppen information på till exempel molntjänstleverantörernas hemsidor. Även andra förhållanden än dålig transparens kan medföra svårigheter vid utredningen av de närmare omständigheterna. Många molntjänstleverantörer har ett extensivt teknologiskt nätverk och ett intensivt informationsflöde. Den geografiska plats på vilken informationen finns kan därför skilja sig åt beroende på vilken dag eller t.o.m. vilket klockslag på dagen man ställer frågan. Processen för behandlingen kan till exempel vara upplagd på det sättet att data som ska behandlas omlokaliseras och behandlas på en ny server som tekniskt sätt är mer lämpad för att utföra den specifika behandlingen, för att sedan föras tillbaka till den ursprungliga servern. I dessa situationer är det viktigt att vara uppmärksam på att även själva överföringarna mellan servrarna utgör en typ av behandling. Behandlingsprocessen sker ofta automatiskt med hjälp av i förväg programmerade algoritmer. Detta kan medföra att även leverantören själv har svårt att kartlägga de närmare omständigheterna i det enskilda fallet och till exempel garantera att informationen finns på en viss geografisk plats vid ett visst tillfälle. Trots svårigheterna är det viktigt att dessa omständigheter klarläggs för att en juridisk utredning av vilka konkreta åtgärder som krävs ska kunna genomföras. Om omständigheterna inte kan klarläggas i ett visst fall torde detta innebära att myndigheten bör avstå från att använda den molntjänsten för den avsedda personuppgiftsbehandlingen.

5.3 LAGLIGHETSPRÖVNINGENS OMFATTNING


Som nämnts i inledningskapitlet tar frågeställningen i den här uppsatsen endast sikte på laglighhetsprövningen av just den reglering som aktualiseras med anledning av att informationen utgörs av personuppgifter. Övriga frågor om bland annat offentlig upphandling och handlingsoffentlighet faller därför utanför frågeställningens omfång. Vid en laglighhetsprövning måste dock alla tillämpliga regelverk beaktas.
5.4 Direkta och indirekta legala hinder

Det finns få legala bestämmelser som medför direkta hinder mot att myndigheter skulle kunna använda molntjänster för personuppgiftsbehandling.110 Vissa bestämmelser medför dock direkta hinder mot viss hantering av personuppgifter, till exempel förbudet mot tredjelandsöverföringar i art. 44 i GDPR. Det finns dock även bestämmelser som ställer upp kvalitativa krav på hur personuppgifter får hanteras, till exempel kravet på att personuppgifter ska omgårdas av en lämplig säkerhetsnivå enligt art. 32 i GDPR. Dessa bestämmelser är ofta formulerade på ett sådant sätt att kraven ökar i paritet med till exempel personuppgifternas känslighet. Detta innebär att ett bestämmande av exakt vilka åtgärder som krävs för att uppfylla kraven måste göras genom en lämpligssäkerhetsbedömning med beaktande av omständigheterna i det enskilda fallet. Bestämmelserna kan innebära så höga krav att den tänkta upphandlingen blir svår att åstadkomma i praktiken. Detta innebär att även de indirekta legala hindren kan medföra att myndigheter tvingas välja bort möjligheten att outsourca personuppgifter för behandling i molntjänster.

5.5 Legala utmaningar

Av analysen ovan framgår att den integritetsskyddsreglering som gäller när myndigheter valt att outsourcing sin personuppgiftsbehandling genom molntjänster inte skiljer sig från vad som gäller om myndigheterna skulle outsourcinga personuppgiftsbehandlingen på något annat sätt. Molntjänster som affärsmodell skiljer sig emellertid från både ITO och IT i egen drift. Skillnaderna i affärsmodellen medför att andra typer av utmaningar uppstår för att möta de krav som integritetsskyddsregleringen ställer.

I ovanstående analys beskrivs också att myndigheter som outsourcingar personuppgiftsbehandling på molntjänster i någon utsträckning måste låta personuppgifterna lagras, bearbetas och överföras med hjälp av hård- och mjukvara som är integrerad med personuppgifterna i en eller flera externa aktörer. I samband med att den faktiska behandlingen övertas av de externa aktörerna förvaltar myndigheter den direkta kontrollen över personuppgifterna vilket ger upphov till nya säkerhetsutmaningar. Vilka rättsliga implikationer detta förhållande får framgår av kapitlet nedan som behandlar personuppgifternas säkerhetsnivå.

Många personuppgifter är skyddade med sekretess. Enligt OSL får myndigheter inte röja sekretessbelagda personuppgifter för bland annat enskilda. Som ovan beskrivits innebär emellertid myndigheters användande av molntjänster att personuppgifterna i viss mån exponeras rent tekniskt när myndigheterna leasar molntjänstleverantörernas tekniska utrustning och programvara. I och med detta uppstår nya utmaningar för att upprätthålla sekretessskyddet. I kapitlet nedan om utlämnande av personuppgifter utreds vilka begränsningar integritetsskyddet medför i sekretessavseende vid myndigheters outsourcing av personuppgiftsbehandling på molntjänster.

5.6 Sammanfattning

Skillnaden mellan laglighetsprövning och lämplighetsprövning kan vara komplext. Inom ramen för laglighetsprövningen av om myndigheter kan outsourcing personuppgiftsbehandling i molntjänster måste olika typer av lämplighetsprövningar göras. Myndigheter har dock även på grund av sin förvaltningsrättsliga självständighet frihet att välja om de finner det lämpligt att personuppgiftsbehandling ska bedrivas i egen regi eller genom outsourcing. Denna allmänna lämplighetsprövning görs efter

---

110 Dataföreningens nätverk Cloud Sweden, Rättsliga frågor vid flytten till molnet – en checklista, v. 1, 2013 (SW35411/12) s. 3 [cit. Cloud Sweden, en checklista]
eget skön med de kriterier och målsättningar som myndigheterna själva bestämmer. Lämplighetsprövningar som görs inom ramen för laglighetsprövningen är emellertid bundna till författningarna vad avser vilka kriterier och mål som bedömningen innefattar.

En laglighetsprövning börjar alltid med att klargöra omständigheterna i den enskilda situationen. Omständigheterna har betydelse för vilka regelverk som ska tillämpas, vilka krav inom regelverken som blir aktuella och hur de kraven ska tolkas. Det kan vara svårt att klargöra omständigheterna, bland annat på grund av att molntjänster ofta har låg transparens i sina verksamheter och på grund av att den tekniska complexiteten bakom molntjänster kan medföra att omständigheterna blir svåra att utreda.

De legala hinder som finns för myndigheter att outsourca personuppgiftsbehandling i molntjänster är ofta indirekta i den meningen att de ställer kvalitetskrav på hur personuppgifterna får hanteras. Kvalitetskraven ökar ofta i paritet med bland annat uppgifternas känslighet vilket i praktiken medför att utmaningarna för att bevara de upphandlade tjänster och medföra att utmaningarna blir svåra att klargöra fallet.

Molntjänster som affärsmodell skiljer sig från ITO och IT-drift i egen regi på flera sätt. Molntjänster medför att myndigheter förstörer den direkta kontrollen över personuppgifterna. Detta innebär att nya legala utmaningar uppstår för myndigheterna att tillgodose integritetsskyddslagstiftningens krav på framför allt personuppgifters säkerhetsnivå, sekretesskydd, skydd från exponering och mot andra länderens rättsordningar. Utmaningar uppstår även för myndigheterna att tillse att externa aktörer faktiskt efterlever de villkor som avtalats. I följande kapitel behandlas var och en av dessa utmaningar.

6 PERSONUPPGIFTERNAS SÄKERHETSNIVÅ


6.1 KRAVET PÅ LÄMPLIG SÄKERHETSNIVÅ

Artikel 32(1) i GDPR ålägger den personuppgiftsansvarige att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifterna. Vad som är en lämplig säkerhetsnivå ska avgöras med beaktande av en rad olika omständigheter som räknas upp i förordningen. De omständigheter som ska beaktas är den senaste utvecklingen, åtgärdernas kostnad och behandlingens art, omfattning, sammanhang och ändamål samt allvaret och sannolikheten bakom riskerna för fysiska personers rättigheter och friheter. Vad som är en lämplig säkerhetsnivå ska enligt art. 32(2) i synnerhet avgöras med beaktande av riskerna för att personuppgifterna odligen skulle förstöras, förloras, ändras eller obehörigen röjas eller åtkommas. Framförallt ska sådana risker beaktas som kan medföra fysisk, materiell eller immateriell skada.111

I artikeln ges även några exempel på vilka åtgärder myndigheter kan vidta och som har betydelse för vilken säkerhetsnivå som omgärda personuppgifterna. Det ålägger myndigheterna att bland annat

111 GDPR, beaktandeskäl 83.
fortlöpande säkerställa uppgifternas konfidentialitet, integritet, tillgänglighet och IT-systemens och IT-tjänsternas motståndskraft och att det går att återställa tillgången till personuppgifterna vid en incident. Det beskrivs även att myndigheterna regelbundet bör se till så att effektiviteten av de åtgärder som vidtagits utvärderas, testas och undersöks. Enligt art. 32(4) ska myndigheterna också säkerställa att alla fysiska personer som har tillgång till personuppgifterna endast behandlar dem enligt instruktioner från myndigheterna.

I art. 25 anges att myndigheterna, utifrån samma skäl som ska beaktas vid vad som är en lämplig säkerhetsnivå enligt art. 32, ska genomföra lämpliga tekniska och organisatoriska åtgärder för att integrera skyddsåtgärderna i själva behandlingen så att dataskyddsprinciper såsom integritet och konfidentialitet iakttas och den enskildes rättigheter skyddas.

Regleringen av personuppgifters säkerhetsnivå i art. 17 i dataskyddsdirektivet och 30-31 §§ i personuppgiftslagen anger på samma sätt som art. 32 i GDPR att lämpliga tekniska och organisatoriska åtgärder ska genomföras för att skydda personuppgifterna från otillåten behandling och att de som har tillgång till uppgifterna endast ska behandla dem enligt instruktioner från den personuppgiftsansvarige. GDPR betonar dock i större utsträckning att man vid lämplighetsbedömningen ska beakta uppgifternas känslighet och sannolikheten och allvaret i riskerna. Förordningen ger fler och noggrannare exempel på vilka konkreta åtgärder som avses. Ingenting tyder på att lagstiftaren genom bestämmelserna i GDPR avser sänka skyddsåtgärder som fördras. Vid bedömningen av vilka krav som ställs i GDPR kan man därför utgå ifrån att de åtminstone motsvarar de krav som ställts i dataskyddsdirektivet och som genomförts i svensk rätt igenom personuppgiftslagen.

För att underlätta bedömningen av vilka konkreta åtgärder som ska vidtas för att uppnå standarden om lämpliga säkerhetsnivå har Datainspektionen skapat ett dokument med allmänna råd om säkerhet för personuppgifter. Dessa rekommendationer reviderades senast i november 2008 vilket innebär att utvecklingen under de senaste tio åren inte beaktats vid utformningen av råden. Av denna anledning bör råden inte användas för att bedöma vilka konkreta åtgärder som är tillräckliga i en viss situation. Råden kan dock fortfarande ge viss ledning i hur myndigheter bör resonera i fråga om vilka uppgifter som förbjuds särskilt skydda och vilka åtgärder som i vart fall inte är tillräckliga.

Det är dock viktigt att minnas att vad som är lämpliga åtgärder i en viss situation inte enbart ska bedömas med beaktaande av uppgifternas känslighet, åtgärdernas kostnader och riskerna utan även utifrån den senaste utvecklingen. Detta innebär att de åtgärder som en gång var lämpliga för en viss situation inte nödvändigtvis lever upp till kraven i en identisk situation som inträder vid ett senare tillfälle. När till exempel tillgänglig teknik på marknaden blivit billigare, den generella hotbildens ökat eller nya rönt om sårbarheter i en viss kryptering, utrustning eller metod uppdagats kan kraven öka. Vad som är lämpliga åtgärder i den särskilda situationen måste slutligen avgöras genom en lämplighetsbedömning av personuppgiftsansvarige myndigheten.

6.2 **Konkreta Åtgärder som Höjer Säkerhetsnivå**

Personuppgifternas säkerhetsaspekter kan klassifieras som antingen fysiska eller logiska.\(^\text{112}\) Den fysiska säkerheten avser de situationer då uppgifterna inte är i rorelse. Fysisk säkerhet rör bland annat frågor om vem som har tillträde till platsen där informationen faktiskt finns, vad personer med tillträde har behörighet att göra på platsen, hur uppgifterna utplånas när de ska tas bort och preventionen av risken för att personuppgifterna stjälts eller slarvas bort. Logisk säkerhet handlar om personuppgifternas säkerhet när de behandlas. Den logiska säkerheten rör till exempel frågor om vem som

\(^{112}\) Ang. detta stycke, se Edvardsson & Frydlinger s. 135 ff.
har tillgång till själva informationen, om någon kan avlyssna informationsflödet eller om ett virus kan kopiera, ändra eller förstöra uppgifterna. Kraven på både den fysiska och logiska säkerheten ska motsvaras av konkreta åtgärder som gemensamt skapar en lämplig säkerhetsnivå.

En lämplig säkerhetsnivå för den fysiska aspekten av säkerheten kan avse åtgärder som till exempel låsutrustning, inpasseringskontroller, galler för fönster, larmutrustning för rök, brand och inbrott, utrustning som skyddar vid störningar i strömtillförseln, kylanläggningar, skydd mot rök och vattendrag, brandsläckningsutrustning, säkerhetssskap och säker placering av IT-utrustningen.\footnote{Ang. detta avsnitt, se Datainspektionens allmänna råd, Säkerhet för personuppgifter, Reviderad november 2008 [cit. DI:s allmänna råd, säkerhet] s. 12 ff.} Kryptering av personuppgifterna är särskilt viktigt om de lagras på portabel IT-utrustning som till exempel laptops. Rutiner kan upprättas för hur utrustningen får användas och hur den ska skyddas.


En behandlingshistorik kan föras för att möjliggöra utredningar av felaktig eller obehörig användning av personuppgifter. Historiken kan programmeras till att vara så detaljerad att den avslöjar vilken åtgärd som vidtagits, det vill säga om åtgärd avsett till exempel läsning, ändring, kopiering eller utplåning av personuppgifter. En sådan logg bör sparas över en viss tid och skyddas mot ändringar av användarna.


När personuppgifter ska utplånas kan detta ske genom att lagringsmedierna förstörs eller, om det inte är möjligt, uppgifterna raderas från lagringsmediet på ett sådant sätt att de inte kan återskapas.
All IT-utrustning bör ha skydd mot skadlig programvara som uppdateras i samband med att programrättelser och andra uppdateringar släpps. En Internetpolicy bör upprättas för alla nätanslutna datorer, särskilt portabla enheter. Regelbundna tester och uppdateringar bör köras för att identifiera hot och brister i utrustningen.

För att hindra otillåten åtkomst av uppgifter kan rutiner upprättas för distansarbete och Internetanvändning, inaktiva användarkonton raderas och modem avstängas när de inte används. Skyddsåtgärder mot avlyssning bör installeras på utrustningen.

De som faktiskt har tillgång till personuppgifterna bör få relevant utbildning och tillgång till en skriftlig sekretesspolicy. Stöd och hjälp vid utrustningens användning kan minska antalet misstag och öka kompetens. Både avsiktlig och oavsiktlig intrång bland personuppgifterna kan ske bland anställda varför det är viktigt att de väsentliga sakerna till vilken det är tillåtet, vilka konsekvenser som kan uppstå och vad som kan öka risken om man bryter mot reglerna och att regler och bestämmelser kunna följas upp.

Det bör även finnas rutiner för uppföljning av säkerhetsincidenter.

6.3 Bedömning av lämplig säkerhetsnivå

Vid upphandling av en molntjänst bör inte myndigheter beskriva vilka tekniska åtgärder som ska vidtas i detalj. Detta kunde leda till att andra likvärdiga tekniska lösningar som myndigheterna inte kände till inte kan användas. En för snåv teknisk specifering riskerar dessutom att snabbt bli obaktad och leda till att de säkerhetsåtgärder som specifiserats istället minskar säkerhetsnivån i jämförelse med andra alternativ. Även om de tekniska åtgärderna inte ska speciferas är det viktigt att myndigheterna är tydliga med vilka krav de ställer på säkerhetsnivån.

Hur myndigheterna bedömer vad som är en lämplig säkerhetsnivå måste myndigheter göra en risk- och sårbarhetsanalys och informationsklassificering. Med hjälp av bland annat den informationen kan myndigheterna utarbeta en kravlista som illustrerar vilken säkerhetsnivå som är lämplig för personuppgifterna i just deras situation.

6.3.1 Risk- och sårbarhetsanalys


114 Myndighet för samhällsskydd och beredskap, Vägledning – Informationssäkerhet i upphandling av system, outsourcing och molntjänster, april 2013 [cit. MSB:s vägledning om informationssäkerhet], s. 25 och 34.

42
Det viktigaste vid en risk- och sårbarhetsanalys är att arbetet sker med tillräcklig kunskap och på ett systematiskt och ordnat vis.\footnote{Ang. följande stycken, se. MSB:s vägledning om informationssäkerhet, s. 28 och DI:s allmänna råd, säkerhet för personuppgifter, s. 15 och Edvardsson & Frydlinger, s. 78.} Analysen ska framförallt bereda myndigheter information om tre övergripande frågor, (1) vilka hot som personuppgifterna kan utsättas för vid den ifrågavarande molntjänsten, (2) vilket allvar som ligger i konsekvenserna av om dessa hot skulle förverkligas (3) hur stor sannolikhet som föreligger för att hoten förverkligas. 

Vid bedömningen av oönskade händelser ska myndigheter kartlägga hotbilden. De ska till exempel bedöma när informationen är sårbar och hur den är sårbar. Vid bedömningen av konsekvenserna måste myndigheter bland annat beakta hur känslig informationen är, hur många personer som informationen rör och vad informationen skulle kunna användas till. Vid bedömningen av sannolikheten ska myndigheter bland annat beakta vem som skulle kunna vara intresserad av informationen, vilka resurser som står dessa personer till förfogande och vilket intresse de har av den.

En risk- och sårbarhetsanalys måste göras för varje leverantör som myndigheterna använder sig av.\footnote{Ang. detta stycke, se MSB:s vägledning om informationssäkerhet, s. 29.} Detta innebär att myndigheterna måste ha helt klart för sig vilka underleverantörer som molntjänstleverantörerna använder sig av och hur detta påverkar säkerhetsnivån som omgärder personuppgifterna. Leveransprocessen hos vissa molntjänstleverantörer kan innebära att personuppgifterna skulle utsättas för en hel kedja av aktörer och aktiviteter innan den slutliga leveransen sker. Alla dessa delar av processen måste beaktas vid risk- och säkerhetsanalysen.

6.3.2 Informationsklassificering

Efter att en risk- och sårbarhetsanalys genomförts bör myndigheter göra en informationsklassning. Vid informationsklassningen ska myndigheter (1) identifiera vilka personuppgifter som är i fråga, (2) klassificera personuppgifternas känslighet och (3) besluta vilken skyddsgränssnitt som krävs för att skydda de specifika typerna av personuppgifter. Vid bedömningen av informationens känslighet och skyddsgränssnitt ska särskilt beaktas konsekvenserna som kan uppstå om de hot som identifierades genom sårbarhets- och riskanalysen förverkligas.\footnote{MSB:s vägledning om informationssäkerhet, s. 30.}

Vilken skyddsgränssnitt som krävs för personuppgifterna beror inte bara på en uppskattning av uppgifternas känslighet utifrån ovanstående kriterier. Lagstiftaren har nämligen kategoriserat vissa personuppgifter som med hänsyn till sitt innehåll ska klassificeras som känsliga. När personuppgifter kan härledas till denna kategori ökar den säkerhetsnivån som kan anses lämplig.

De personuppgifter som lagstiftaren identifierat som känsliga återfinns i art. 9 i GDPR. Där fastställdes att sådana uppgifter som ”avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemsskap i fackförening, ---genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning”. De personuppgifter som inte klassas som känsliga personuppgifter beror inte bara på en uppskattning av uppgifternas känslighet utifrån ovanstående kriterier. Lagstiftaren har nämligen kategoriserat vissa personuppgifter som med hänsyn till sitt innehåll ska klassificeras som känsliga. När personuppgifter kan härledas till denna kategori ökar den säkerhetsnivån som kan anses lämplig.

Det finns många olika typer av personuppgifter som inte klassas som känsliga personuppgifter enligt art. 9 men som enligt lagstiftaren fortfarande har ett högre skyddsvärde än vanliga personuppgifter. I den här uppsatsen benämns dessa personuppgifter i klump som ”integritetskänsliga personuppgifter”. Uppgifter om ekonomisk hjälp inom socialtjänsten, enskildas personliga och ekonomiska förhållanden inom bank- och försäkringsväsendet, uppgifter inom kreditupplysning eller inkassoöverenskommelse är normalt att anse som integritetskänsliga uppgifter.\footnote{DI:s allmänna råd, säkerhet för personuppgifter under rubriken ”Säkerhetsnivå” s. 18.} Integritetskänsliga personuppgifter...
omfattar emellertid även många andra typer av upplysningar. Att en uppgift skyddas av sekretess i OSL är en indikation på att personuppgiften är att se som integritetskänslig. Beroende på bland annat sammanhanget i vilket uppgiften förekommer kan dock även andra uppgifter förtjäna ett högre skydd på grund av att de är integritetskänsliga.

Personuppgifter som vanligen inte är att betrakta som integritetskänsliga personuppgifter är uppgifter som till exempel rör medlemskap, anställningsförhållanden, kundförhållanden och därmed jämförliga förhållanden.

Det är viktigt att komma ihåg att en personuppgifts legala kategorisering utifrån dess innehåll inte är den enda faktorn av betydelse vid en bedömning av hur hög skyddsnivå som är lämplig för uppgifterna. En mängd vanliga personuppgifter om en och samma person kan, beroende på hur detaljerat bild som kan erhållas av personen i fråga, vara lika skyddsvärda som enstaka känsliga uppgifter. Ytterligare en faktor av betydelse för hur hög skyddsnivå som ska omgärda personuppgifterna är hur många personer som personuppgifterna innehåller upplysningar om. Organiseringen av personuppgifter i olika kategorier är alltså inte ensamt utslagsgivande för vilken skyddsnivå som krävs utan en indikation på vilken typ av uppgifter som redan på grund av sitt innehåll kräver en högre skyddsnivå.

6.4 LÄMPLIG SÄKERHETSNIVÅ OCH OLKA MOLTNTJÄNSTER

När myndigheter har underrättat sig om vilka omständigheter som föreligger i just deras situation och bedömt vilken skyddsnivå personuppgifterna lämpligen bör ha kan myndigheter ställa upp de legala krav som gäller i den specifika situationen. Vid användningen av molntjänster finns sällan personuppgifterna under myndigheternas direkta kontroll. Den faktiska personuppgiftsbehandlingen sker ofta automatiskt med molntjänster leverantörernas utrustning och under överinseende av molntjänstleverantörernas personal. Trots detta är myndigheterna som personuppgiftsansvariga rättsligt skyldiga att se till att de åtgärder som krävs faktiskt vidtas.


Vissa teknologiska och ekonomiska faktorer som inte ska kommenteras närmare här har lett till att marknadskoncentrationen bland molntjänstleverantörer är hög. Ofta är leverantören en betydligt större organisation än de enskilda kunderna, även när dessa utgör av myndigheter. Detta marknadsförhållande innebär att partsställningen i förhandlingarna gällande molntjänstavtalet sällan är särskilt jämliga. För kunden innebär leverantörens allmänna villkor ofta en ”take it or leave it” situation. Möjligheterna till flexibilitet i förhandlingarna försämras också av att tjänsten hos leverantörerna ofta är standardiserad för att möjliggöra automatisering. Om leverantören förhandlar med kunderna om separata och varierande avtalsvillkor förtas de stordriftsfördelar som molntjänster som affärssmodell bygger på. För att kunden ska kunna nyttja tjänsten måste den därför ofta acceptera att det är

121 DI:s allmänna råd, säkerhet för personuppgifter, s. 18.
122 DI:s allmänna råd, säkerhet för personuppgifter, s. 18.
leverantören som dikterar villkoren. Det förhållandet att förhandlingsställningen är ojämlik innebär dock inte att myndigheterna slipper ifrån sitt legala ansvar. Myndigheterna måste alltid ta ansvaret för att upphandlingen av molntjänsten grundas på ett molntjänstavtal där de legala kraven motsvaras i villkoren och kan kontrolleras på ett tillfredsställande sätt.

Molntjänsternas särskilda karaktär innebär att myndigheter som nyttjar dem alltid kommer tvingas överlämna en viss del av säkerhetskontrollen till molntjänstleverantörerna. Myndigheter kan inte behålla all kontroll genom att till exempel reglera det i avtalet. Sådana villkor skulle innebära att vinsterna med tjänsten inte kan uppnås och att molntjänstens tekniska egenskaper i form av bland annat skalbarhet och elasticitet går förlorade. Om myndigheter inte kan lämna ifrån sig vissa delar av säkerhetskontrollen måste myndigheterna därför välja ett annat upplägg för sin verksamhet än outsourcing genom molntjänster.


Möjligheterna för myndigheter att påverka säkerhetsnivån genom avtalsvillkor är störst vid privata moln som levereras med IaaS. I dessa moln kan myndigheter nämligen ofta reglera till exempel var datorhallen ska ligga och vilken utrustning och programvara som ska användas i avtalet med molntjänstleverantörerna. De säkerhetsmässiga kraven torde därför vara lättare att uppfylla vid privata moln. Dessa typer av avtal medför dock ett högre ansvar för myndigheterna. Ansvaret kan minska molntjänstens attraktivitet eftersom vinsten med molntjänster i stora delar bygger på att ansvaret för IT-funktioner övertas av molntjänstleverantörerna.


123 Ang. detta stycke, se Edvardsson & Frydlinger s. 82 f.
124 Ang. detta stycke se Edvardsson & Frydlinger s. 82 ff.
vilka medför att separationen av åtkomst mellan kundernas information inte bevaras är större vid publika molntjänster än vid andra leveransmodeller.\textsuperscript{126} Publika molntjänster bör av bland annat ovanstående skäl inte användas för andra typer av information än sådan som kräver en låg säkerhetsnivå.\textsuperscript{127}


Det går inte att göra ett generellt uttalande om huruvida det är möjligt för myndigheter att outsourca personuppgiftsbehandling i molntjänster utifrån kraven på lämplig säkerhetsnivå. Möjliheterna måste istället utredas i det enskilda fallet utifrån de ovan angivna omständigheterna. Kravet som uppställs i GDPR om en lämplig säkerhetsnivå utgör inte ett direkt hinder för myndigheter att anlita privata leverantörer av molntjänster eftersom kravet på en lämplig säkerhetsnivå stiger paritet med de ovan redovisade faktorerna. Kravet innebär även att molntjänster med mindre säkra typer av leveransmodeller och tjänstemodeller som endast erbjuder en låg säkerhetsnivå sällan kan användas. Eftersom högre krav på säkerhetsnivån ofta gör att möta genom organisatoriska eller tekniska åtgärder blir frågan om en specifik personuppgiftsbehandlingen kan outsourcas i en molntjänst i slutändan ofta en kostnadsfråga. Kravet på en lämplig säkerhetsnivå utgör dock ett direkt hinder i de fall personuppgifterna har ett mycket högt säkerhetsbehov och av den anledningen i praktiken inte kan behandlas i molntjänster.\textsuperscript{128}

6.5 Sammanfattning

Personuppgiftsansvariga myndigheter är förpliktade att omgärda personuppgifter med en lämplig säkerhetsnivå. Vad som är en lämplig säkerhetsnivå avgörs med beaktande av den senaste utvecklingen, skyddsåtgärdernas kostnad, behandlingens art, omfattning och ändamål samt allvaret i konsekvenserna och sannolikheten för förverkligande av riskerna för de registrerade personernas rättigheter och friheter som behandlingen medför. I myndigheternas ansvar ingår att integrera skyddsåtgärder i själva utformningen av personuppgiftsbehandlingen och att kontinuerligt utvärdera, testa och undersöka effektiviteten i de vidtagna åtgärderna.

\textsuperscript{126} Edvardsson & Frydlinger, s. 77.
\textsuperscript{127} Se Europeiska unionens byrå för nät- och informationssäkerhet, Information Assurance Framework, november 2009, kapitel 5.1 under ”Note to governments”.
\textsuperscript{128} MSB:s vägledning om informationssäkerhet, s. 22 f.
Både personuppgifternas fysiska och logiska säkerhet bör skyddas med tekniska och organisatoriska åtgärder. Den fysiska säkerheten kan till exempel skyddas genom tillträdskontroller och larm- och låsutsnittning. Den logiska säkerheten kan skyddas genom bland annat behörighetskontroller, behandlingshistorik, säkerhetskopiering och skydd mot skadlig programvara. Uppgifterna kan även skyddas genom organisatoriska åtgärder, till exempel genom utarbetande av rutiner för Internetanvändning och distansarbete och genom att förse anställda med relevant utbildning.


När myndigheter använder sig av molntjänster för personuppgiftsbehandling förblir de ansvariga trots att de förlorar den direkta kontrollen av personuppgifterna. Myndigheter kan dock skydda personuppgifterna både genom att välja vilken molntjänstleverantör som ska användas och genom att reglera skyddsnivån i avtalen med molntjänstleverantören. Om avtalen i ett enskilt fall inte speglar den skyddsnivå som framgår av kradlistan kan inte myndigheter lagligen använda den molntjänsten för den avsedda personuppgiftsbehandlingen.

Möjligheterna för myndigheter att förhandla om villkoren kan ofta vara små, bland annat för att molntjänstleverantörernas organisationer ofta är stora, för att molntjänsterna är standardiserade för att möjliggöra automatisering och för att separata villkor för olika kunder ofta innebär att vinsterna med molntjänster som affärsmodell förtas.

Eftersom kravet på personuppgifternas säkerhetsnivå stiger i paritet med bland annat personuppgifternas känslighet är personuppgifter med en hög känslighet mindre lämpade för behandling i molntjänster. Kraven på säkerheten i molntjänsterna kan dock mötas med säkerhetsbehövande åtgärder varför frågan om myndigheter kan behandla personuppgifterna i molntjänsterna ofta blir en kostnadfråga. Om myndigheter inte finner det lämpligt att överlämna säkerhetsarbetet i ett visst fall kan dock inte molntjänster användas.

Möjligheterna att påverka säkerhetsnivån genom avtal med molntjänstleverantörerna är som störst vid molntjänster med privata moln. Med dessa moln riskerar nämligen inte myndigheternas önskemål rörande avvägningen mellan risk och kostnad att stå i strid med andra kunders önskemål. Molntjänstleverantörer har därför möjlighet att anpassa tjänsten utifrån myndigheternas önskemål i större grad.

IaaS och PaaS innebär att myndigheten har större kontroll över vilken programvara som ska användas. Av den anledningen kan myndigheten anpassa valet av programvara så att det inkluderar säkerhetsfunktioner som varar mot myndighetens behov. Även den underliggande strukturen, vilken molntjänstleverantörerna ansvarar för, kan dock medföra säkerhetsrisker varför de måste analyseras och regleras i avtalen. SaaS innebär att myndigheten har mindre möjligheter att påverka säkerhetsnivån genom avtalen. Detta innebär dock inte att SaaS alltid har en lägre säkerhetsnivå.

Säkerheten i olika molntjänster skiljer sig inte beroende på deras tjänst- och leveransmodeller. Processen bakom den slutliga leveransen har också betydelse, särskilt vad avser underleverantörer och den geografiska spridningen av molntjänstleverantörernas servern. Att generellt uttala sig om huruvida myndigheter kan använda molntjänster för personuppgiftsbehandling försvårar ytterligare av faktorn att det legala kravet på en lämplig säkerhetsnivå stiger i paritet med uppgifternas känslighetsnivå. Bedömningen av om molntjänster kan användas av myndigheterna för personuppgiftsbehandling måste därför göras i det enskilda fallet. Personuppgifter med ett mycket högt säkerhetsbehov torde dock inte kunna hanteras via molntjänster.

7 ÖVERLÄMNANDE AV PERSONUPPGIFTER

När myndigheter anlitar molntjänstleverantörer för personuppgiftsbehandling måste personuppgifterna överlämnas till molntjänstleverantörerna för att dessa ska kunna utföra den avsedda behandlingen. Om myndigheterna av legala skäl inte kan överlämna vissa typer av personuppgifter till molntjänstleverantörerna är detta ett direkt hinder för myndigheterna att outsourca personuppgiftsbehandling i molntjänster. I det här kapitlet ska utredas i vilken utsträckning sekretessbestämmelserna hindrar myndigheter från att anlita molntjänstleverantörer för personuppgiftsbehandling.

7.1 PERSONUPPGIFTER UTAN SEKRETESS

Som tidigare beskrivits har molntjänstleverantörer rättslig status som personuppgiftsbiträden enligt art. 4(8) i GDPR. I egenskap av personuppgiftsbiträden ska molntjänstleverantörer inte beaktas som tredje part när förordningen tillämpas, art. 4(10). Att molntjänstleverantörer inte ska betraktas som tredje part innebär bland annat att de inte behöver ha en egen från myndigheterna separerad laglig grund för att behandla personuppgifterna. För myndigheten gäller dock det grundläggande kravet på att all personuppgiftsbehandling bara får ske med rättsligt stöd enligt art. 6(1) oavsett om de använder ett personuppgiftsbiträde eller ej. Myndigheter kan sålunda överlämna personuppgifter som inte är sekretessreglerade till personuppgiftsbiträden så länge de har en legitim grund för behandlingen av personuppgifterna.

Trots att molntjänstleverantörer inte är tredje part är ett överlämnande av personuppgifterna till molntjänstleverantörer en form av personuppgiftsbehandling. Som ovan beskrivits tolkas begreppet personuppgiftsbehandling brett och tillhandahållande av personuppgifter utgör en personuppgiftsbehandling på vilket sätt det än sker. Även om molntjänstleverantörer inte är tredje part är de fortfarande att betrakta som mottagare vid ett överlämnande av personuppgifter varför ett tillgängliggörande av uppgifterna för personuppgiftsbiträdet utgör en behandling, art. 4(9).

I art. 28(3.a) i GDPR anges att det i avtalen mellan myndigheter och molntjänstleverantörer ska föreskrivas att behandling enbart får utföras av molntjänstleverantörerna enligt dokumenterade instruktioner från myndigheterna. Av denna avtalsklausul följer en civilrättslig tystnadsplikt för molntjänstleverantörerna. Molntjänstleverantörerna ska även säkerställa att personal som behandlar personuppgifterna har ingått avtal om tystnadsplikt. Enligt art. 28(4) ansvarar molntjänstleverantörer för att
deras egna underleverantörer genom avtal åläggs samma skyldigheter som de själva har gentemot den personuppgiftsansvarige. Av detta följer att även underleverantörer kommer lyda under en civilrättslig tystnadsplikt.

7.2 INNEBÖRDEN AV SEKRETESS


Enligt 2 kap. 1 § OSL gäller förbudet att röja sekretessbelagda personuppgifter för myndigheter och personer som fått kännedom om uppgifterna genom att delta i myndighetens verksamhet för det allmänna räkning. De personer som avses är anställda eller uppdragstagare hos myndigheter eller de som deltagit i ett myndighets verksamhet på grund av tjänsteförmåner eller annan liknande grund. 8 kap. 1 § OSL framgår att förbudet innebär att informationen inte får lämnas ut till varken enskilda eller andra myndigheter som inte omfattas av den legala tystnadsplikten i OSL eller en tystnadsplikt i någon annan lag vilken OSL hänvisar till. Sekretesssen behöver sålunda vara beaktas i de situationer då uppgifterna lämnas ut till någon som inte omfattas av en sådan tystnadsplikt.

Anställda hos organisationer utanför myndigheten kan i undantagsfall omfattas av tystnadsplikten. Anställda hos personuppgiftsbiträden omfattas emellertid inte eftersom de representerar ett rättsobjekt som är externt i förhållande till myndigheten. Relationen mellan privata molntjänsterleverantörer och myndigheter har affärsmässig prägel och de kan därför inte sågas delta i myndighetens verksamhet. Anställda hos den personuppgiftsansvarige har inte sitt uppdrag och sin rapporteringsskyldighet i förhållande till myndigheten utan i förhållande till den som är ansvarig hos den personuppgiftsansvarige.

7.3 SEKRETESSPRÖVNING


Om det föreligger absolut sekretess får myndigheten bara lämna ut uppgiften i de fall det finns en sekretessbrytande bestämmelse. De sekretessbrytande bestämmelserna finns i framför allt 10 kap. OSL. Några sekretessbrytande bestämmelser som är intressanta vad avser möjligheterna att outsource personuppgifter i molntjänster behandlas i avsnitten nedan.


7.4 Schabloniserad sekretessprövning
Vid en outsourcing av myndigheters personuppgiftsbehandling i molntjänster är det ofta inte praktiskt möjligt att sekretesspröva varje uppgift för sig. När en stor mängd uppgifter ska sekretessprövas kan prövningen i vissa enklare situationer göras genom ett så kallat schabloniserat förfarande. När myndigheter inte kan bilda sig en uppfattning om risken avseende varje enskild uppgift kan kunskap om mottagarens identitet och avsikt med uppgifterna i förening med bedömning av vilken risk som typiskt sett föreligger för uppgifternas slag ge tillräckligt underlag vid bedömningen. Det torde därför vara möjligt för myndigheter att lämna ut uppgifterna till molntjänsteleverantörer i de enkla fall då en schabloniserad sekretessprövning kan göras. Vissa omständigheter medför emellertid att det ofta är svårt för myndigheter att genomföra en schabloniserad sekretessprövning för utlämnande till molntjänsteleverantörer. Sekretessprövningen måste göras mot alla som personuppgifterna utlämnas till, vilket kan medföra att många personer bland molntjänsteleverantörens personal omfattas av prövningen. Om molntjänsteleverantörerna anlitat underleverantörer som kan komma att få tillgång till informationen måste prövingen även ske

130 Bohlin s. 177 f.
131 JO:s beslut den 9 september 2014, dnr 3032-2011.
132 Dir. 2009:19.
133 eSams vägledning om sekretess, s. 24.
134 Prop 1980/79:2, del A, s. 81.
135 Pensionsmyndigheten, Molntjänster i staten, bilaga 1, s. 10 f.
mot underleverantörernas personal. Ytterligare omständigheter som kan försvåra prövningen är att servrarna på vilka personuppgifterna kommer behandlas och personerna som kan komma att få tillgång till uppgifterna kan finnas i olika länder.

Dessa praktiska svårigheter torde i praktiken göra en att myndigheter ofta inte kan lämna ut sekretessreglerade personuppgifterna till molntjänstleverantörer med en schabloniserad sekretessprövning. Möjheterna till sådana prövningar torde vara begränsade till sekretessuppgifter med ett rakt skaderekvisit till nationella aktörer med lågt personalantal och få eller inga underleverantörer.

7.5 NOVDÄNIGT FÖR ATT FULLGÖRA MYNDIGHETENS VERKSAMHET

Sekretess kan brytas när ett utlämnande av uppgifterna är nödvångigt för att myndigheter ska kunna fullgöra sin verksamhet, 10 kap. 2 § OSL. Myndigheters verksamhet består av de uppgifter som följer av myndighetsinstruktionerna och andra lagar och förordningar, myndigheternas regleringsbrev och särskilda regeringsbeslut. Frågan är om effektivitets- och kostnadsskäl som molntjänster medför kan anses tillräckliga för att utlämnande till molntjänstleverantörer ska vara nödvändig i den mening som avses i 10 kap. 2 § OSL.

Bestämmelsen infördes i svensk rätt genom 1 kap. 5 § i den idag upphävda sekretesslagen (1980:100). Av lagrådets yttrande i förarbetena till sekretesslagen, vilket det föredragande statsrådet anslöt sig till, framgår att bestämmelsen ska tillämpas restriktivt. Sekretess kan bara åsidosättas då det är en nödvändig förutsättning för fullgörandet av myndighetens åligganden. I förarbetena står att ”[b]lott och bart en bedömning att effektiviteten i myndighetens handlande nedsätts genom en föreskriven sekretess får inte leda till att sekretessen åsidosätts.”

År 2015 publicerade E-delegationen en förstudie om sekretess och outsourcing där man uttalade att det finns anledning att frångå dessa uttalanden. I förstudien påstod att den sekretessbrytande bestämmelsen i 10 kap 2 § OSL förlorar sin praktiska betydelse när den tolkas så snävt att en effektivisering inom förvaltningen inte kan anses nödvändig. E-delegationen menade att en restriktiv tillämpning av bestämmelsen inte innebär detsamma som att bestämmelsen bara ska tillämpas i undantagsfall. I studien hävdades även att en så snäv tolkning inte stämmer väl överens med tolkningen av bestämmelsen i andra sammanhang. E-delegationen hänvisar med anledning av detta argument bland annat till ett annat uttalande i förarbetena till sekretesslagen där det står att bestämmelsen kan användas för att bryta sekretessn eller medfört av utomstående experter. I förarbetena står det att det ”[i] särskilda fall kan --- vara nödvändigt för en tjänsteman att vända sig till en utomstående expert och att däri vid upplys känsmo om omständigheterna”.

eSams vägledning om sekretess, s. 27 f.

---

136 Pensionsmyndigheten, Molntjänster i staten, bilaga 1, s. 7 under rubriken ”Schabloniserad skadeprövning vid massutlämnande” och s. 10 f.
137 Prop. 1979/80:2, del A, s. 465 och s. 494.
139 eSams vägledning om sekretess, s. 27 f.
Frågan huruvida effektivitetsbänsyn ska kunna beaktas vid bedömningen av vad som är nödvändigt aktualiserades vid ett tillsynsreerande hos JO.\textsuperscript{140} I ärendet riktade JO kritik mot vissa offentliga vårdgivare för att de ingått avtal om journalföring med ett företag. Uppgifterna som den privata aktören fått i uppdrag att föra in i journalerna var sekretessreglerade med ett omvänt skaderekvist och fick inte röjas utan att myndigheten vid en sekretessprövning bedömt att det stod klart att uppgifterna kunde lämnas ut utan att en viss skada uppstod. Vårdgivarna hävdade att den ifrågavarande sekretessbrytande bestämmelsen i 10 kap 2 § OSL möjliggiordde ett utlämnande på grund av att det var nödvändigt för att de skulle kunna fullfölja sitt uppdrag. JO menade emellertid att en effektivisering inte innebär att åtgärden var nödvändig i den mening som avses i 10 kap 2 § OSL. JO konstaterade att bestämmelsen ska tillämpas restriktivt och därför i praktiken bara blir tillämplig i undantagsfall.

I doktrinen har framhållits att ingen erinran lämnades mot lagrådets yttrande vid bestämmelsens innehåll och att intresse i den givna verksamheten inte var avsedd. JO:s beslut den 9 september 2010 menade emellertid att en effektivisering är nödvändig för att myndigheten ska kunna fullgöra visst åliggande och att effektivitetskär inte är tillräckliga.\textsuperscript{142}

eSams uttalande görs inte de lege ferenda utan ger uttryck för medlemmarnas rättssuppfattning. eSam gör dessutom uttalandet i ett sammanhang som gör anspår på att vara vägledande för myndigheter.\textsuperscript{143} Enligt den svenska rättskalleläran har varken eSams eller JO:s uttalanden någon teoretiskt normerande verkan även om båda aktörerna torde ha förhållandevis stor normerande verkan i praktiken. Uttaidanen i förarbeten ges dock traditionellt sett betydelse vid uttolkningen av lagtext eftersom de uttrycker lagstiftnares subjektiva vilja. Särskild tyngd läggs vid förarbetsuttaidanen då de inte stöd i doktrinen. Vid tolkningen av rättsläget är dock utgångspunkten lagtextens ordalydelse.


Eftersom myndighetens uppdrag och förmåga att utföra uppgifter skiljer sig åt beroende på de närmar omständigheterna kan inte frågan om myndigheter lagligen kan outsourcing sekratessbelagda personuppgifter med stöd av 10 kap. 2 § OSL besvaras på ett generellt plan. När frågan är aktuell måste den istället utredas och besvaras i den enskilda situationen. Sannolikt är dock frekvensen med

---

\textsuperscript{140} JO:s beslut den 9 september 2014, dnr 3032-2011.
\textsuperscript{141} Ahlström, Offentlighets- och sekretesslag (2009:400), Lexino, 19 november 2016, 10 kap. 2 §, Lexino 2017-05-01.
\textsuperscript{142} Bohlin, s. 200 f och Lenberg, Eva, Geijer, Ulrika, Tansjö, Anna, Offentlighets- och sekretesslagen - en kommentar, Zeteo, den 24 november 2017, kommentaren till 10 kap 2 § OSL, fr.o.m. stycket som börjar ”Bestämmelsen i denna paragraf”.
\textsuperscript{143} eSams vägledning om sekretess, faktaruta på s. 2 och s. 3.
vilken myndigheter finner sig i en sådan ansträngd situation att paragrafen kan tillämpas mycket li-
att outsource vissa tekniska arbetsuppgifter som innebär att sekretessbelagd information blir tekniskt tillgänglig för tjänsteleverantörer. De beskriver att ”avsikten med ett sådant tillgängliggörande -- inte [är] att mottagaren ska tillgodogöra sig informationsinnehållet. Vid outsourcing av till exempel it-drift, scanning eller kommunikationstjänster är syftet istället att mottagaren ska tekniskt bearbeta själva informationsmassan, oavsett dess innehåll. Enligt eSams mening finns det därför, i vart fall i dessa sammanhang, skäl att överväga en nyanserad tolkning av offentlighets- och sekretesslagens röjandebegrepp.

Till stöd för sin tolkning av begreppet röjande lyfter eSam ett brottmålsprejudikat från Högsta domstolen.\(^{149}\) I målet har Högsta domstolen uttalat sig närmare om innebörden av begreppet med anledning av ett åtal rörande vårdslöshet med hemlig uppgift enligt 19 kap 9 § brottsbalken. Högsta domstolen konstaterade i sitt avgörande att ett tekniskt tillgängliggörande av uppgiften inte var tillräckligt för att utdöma straffansvar. Det krävdes också att omständigheterna varit sådana att man måste räkna med att den obehörige kommer ta del av uppgiften. eSam lyfter ett uttalande i förarbetena till den idag upphävda sekretesslagen till stöd för sin tolkning.\(^{150}\) I förarbetena ges exempel på hur uppgifter kan röjas genom att ”allmän handling företes” eller att ”förevisa ett hemligt föremål”. Enligt eSam indikerar formuleringen att det krävs att mottagaren tar del av eller åtminstone har rätt att ta del av uppgifterna.

Med eSam tolkning av begreppet skulle myndigheter sålunda kunna anlita molntjänstleverantörer för personuppgiftsbehandling av sekretessreglerade personuppgifter under vissa förutsättningar. Först och främst får inte molntjänstavtalet medföra att molntjänstleverantörernas personal måste ta del av de sekretessreglerade personuppgifterna för att kunna tillgodose molntjänstleverantörernas skyldigheter. Syftet med det tekniska tillgängliggörandet får nämligen inte vara att de ska tillgodogöra sig informationsinnehållet. Det måste dessutom föreligga omständigheter som medför att det är osannolikt att personalen faktiskt tar del av informationsinnehållet. Detta ”rekvisit” kan enligt eSam uppfyllas genom att avtalen mellan myndigheter och molntjänstleverantörer reglerar att molntjänstleverantörerna ska ingå avtal med sina anställda om att de inte får ta del av, sprida eller utnyttja personuppgifterna.

eSams tolkning av begreppet röjande kan kritiseras utifrån den lagtolkningsmetodologi som använts. eSam ger i sin argumentation uttryck för en radikal syn på rättsutvecklingen genom att använda sig av så kallade objektivt teleologiska argument. Dessa resonemang tar utgångspunkt i vilken tolkning av ett obestämt uttryck som ger den bästa samhälleliga effekten. Argumenten grundar sig i intressen som uppstått efter att lagen stiftats vilka inte kan tillgodoses eller vars funktionalitet reduceras med anledning av att lagstiftaren inte hunnit (eller velat) behandles frågan i ny lagstiftning. Denna lagtolkningsmetod är kontroversiell och bör därför användas med försiktighet.

Även eSams hänvisning till Högsta domstolens avgörande går att kritisera. Målet som refererades är ett brottmål, vilket medfört att legalitetsprincipen gjort sig särskilt starkt gällande. Inom strafflagstiftningen ska begrep och uttryck tolkas strikt inom dess ordalydelse för att rättssäkerheten ska upprätthållas. Tolkningen av begrepp inom strafflagstiftningen har därför inte nödvändigtvis båring på hur begreppen ska förstås inom andra rättssammanhang. Vid tolkningen av förvaltningsrättslig lagtext finns det ofta skäl att tolka bestämmelser som ålägger det allmänna skyldigheter på ett extensivt sätt om det kan medföra ett ökat rättssäkerhetsskydd för enskilda. Vad avser eSams refererade uttalande i förarbetena till sekretesslagen har jag ingen annan invändning än att det inte framgår annat i

\(^{149}\) NJA 1991 s. 103.  
\(^{150}\) Prop. 1979/80:2, del a, s. 119.
förarbetena än att formuleringen uttrycker exempel, inte rekvisit, på når en uppgift ska anses röjd och att det av uttalandet framgår att exempen inte är uttömmande.

Efter denna kritik av eSam:s uttalanden ska understrykas att frågan om röjandebegreppets räckvidd inte är avgjord och att eSam, trots bristerna i den juridiska argumentationen, kan ha gjort en riktig bedömning av rättsläget. Varken förarbetutsutalandena eller det refererade brottmålet kan tolkas som att betydelsen av begreppet röjande i sekreteringslagen är inskränkt till att endast avse de situationer då mottagaren faktiskt tagit del av eller haft en rättslig möjlighet att ta del av informationen. Även om frågan inte är slutligt avgjord bör myndigheter av rättssäkerhetsskäl förhålla sig för- siktiga till tolkningar av rättsläget som kan leda till ett sämre skydd för enskilda.

7.8 **PERSONUPPGIFTER SOM RÖR HÄLSA**

I vissa situationer gäller särskilda regler vid utlämnande av känsliga personuppgifter som rör hälsa. I dessa situationer får nämligen behandlingen bara ske av, eller under ansvar av, en yrkesutövare som lyder under en legal tystnadspflicht, art. 9(3) i GDPR.

Med personuppgifter som rör hälsa avses ”hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetsk Capacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg för förvaltning av hälso- och sjukvårdsstjänster och social omsorg”. Detta innebär att i princip alla personuppgifter som förekommer inom hälso- och sjukvården omfattas.\(^\text{151}\)

De särskilda reglerna tar endast sikte på sådana situationer då hälsouppgifterna behandlas med stöd av rättsgrunden i art. 9(2.h) om att det är nödvändigt av hänsyn till ett allmänt intresse.


7.9 **PERSONUPPGIFTER SOM RÖR LAGÖVERTRÄDELSER**

Personuppgifter som innefattar upplysningar om brott, misstanke om brott eller straffprocessuella tvångsmedel betraktas inte som känsliga personuppgifter. Enligt art. 10 i GDPR får dock sådana personuppgifter endast behandlas ”under kontroll av myndighet” eller med stöd av legala bestämmelser som fastställer lämpliga skyddsåtgärder.

Uttrycket ”under kontroll av en myndighet” ska inte tolkas så vidsträckt att det omfattar privata aktörer som står under tillsyn av datainspektionen.\(^\text{152}\) Bestämmelsen syftar till att säkerställa att det finns en tillämplig reglering som ger uppgifterna ett tillräckligt gott skydd. Detta innebär att personuppgiftsbehandling av lagöverträdelser får utföras av enskilda under förutsättning att en myndighet är personuppgiftsansvarig. Av den anledningen kan myndigheter outsourcinga personuppgiftsbehandling som rör lagöverträdelser genom molntjänster så länge de vidtar tillräckliga åtgärder för att skydda de personer vilka personuppgifterna rör.

---

\(^{151}\) GDPR, beaktandeskäl 53.

\(^{152}\) För följande diskussion, se Prop 2017/18:105 s. 99 f.
Vad som är tillräckliga åtgärder i det enskilda fallet måste myndigheten avgöra från fall till fall. Datainspektionen har dock uttalat att sådana personuppgifter åtminstone ska skyddas med samma säkerhetsnivå som känsliga personuppgifter.153

7.10 SAMMANFATTNING

För att myndigheter ska kunna outsourca personuppgiftsbehandling i molntjänster måste personuppgifterna överlämnas till molntjänstleverantörerna så att dessa ska kunna utföra den avsedda behandlingen. Molntjänstleverantörer är inte tredje part varför de kan behandla uppgifterna utan att ha en från myndigheten separerad laglig grund för behandlingen.

När personuppgifter är skyddade av sekretess får myndigheter ofta inte röja dem för molntjänstleverantörer. Vilka personuppgifter som är föremål för sekretessreglering framgår av bland annat OSL. Sekretessreglerade personuppgifter får röjas av myndigheten om det finns en tillämplig sekretessbrytande bestämmelse. Uppgifter som skyddas av skaderekviser får även röjas om myndigheten funnit att så kan ske efter en sekretessprövning. Vid en sekretessprövning ska beaktas vilken skaderisk uppgifter av ifrågavarande slag typiskt sett medför vid ett utlämnande och hur uppgifterna i den särskilda situationen kommer hanteras, vilken spridningsrisk som föreligger och om mottagaren lyder under tystnadsplikt.

Civilrättsliga tystnadsplikter har inte samma tyngd som straffsanktionerade tystnadsplikter. Särskilt integritetskänsliga uppgifter kan inte lämnas ut om mottagaren inte lyder under en straffsanktionerat tystnadsplikt.

När myndigheter ska outsourcingar i molntjänster är det sällan möjligt att sekretesspröva uppgift för sig, varför endast ett schablonartat förfarande som kan komma ifråga. På grund av molntjänstemännen karaktär är dock sådana förfaranden sällan möjliga att genomföra. Huruvida ett schablonmässigt förfarande kan användas av myndigheten beror bland annat på hur många som är anställda hos molntjänstleverantören och dess eventuella underleverantörer som kommer få del av uppgifterna och om dessa personer befinner sig inom svensk jurisdiktion.

När ett utlämnande av uppgifter är nödvändigt för att myndigheter ska kunna fullgöra sin verksamhet kan sekretess brytas. Outsourcing av personuppgiftsbehandling i molntjänstleverantörer medför framförallt kostnadsmässiga och effektivitetsmässiga vinster för myndigheterna. Sådana vinster kan dock inte beaktas annat än i en mycket begränsad utsträckning vid bedömningen av om utlämnandet är nödvändigt.

Sekretessen för uppgifter som skyddas av skaderekviser får brytas om myndigheter fattar beslut om att den enskilde som tar del av uppgiften ska omfattas av en straffsanktionerad tystnadsplikt. Sådana beslut måste dock föregås av en prövning i varje enskilt fall och kan bara angå fysiska personer. Beslutet får dessutom inte fattas i förväg för en viss typ av information. Av dessa anledningar är inte denna sekretessbrytande bestämmelse lämpad för myndigheter som vill outsourcingar personuppgiftsbehandling i molntjänster hos en privat molntjänstleverantör.

Det är troligen inte möjligt för myndigheter att outsourcingar sekretessbelagda personuppgifter för behandling i molntjänster utan att uppgifterna röjs för molntjänstleverantörerna. eSam har dock föreslagit att ett tekniskt tillgängliggörande med avseende på uppgifterna inte innebär att de är röjda om mottagaren inte har rättsliga möjligheter att faktiskt ta del av informationsinnehållet och om omständigheterna talar för att det är osannolikt att så kommer ske. Den juridiska tyngden bakom argumenten till denna

---

153 DI:s allmänna råd, säkerhet för personuppgifter, s. 18 f.
tolkning är förhållandevis svag och speglas inte i de traditionella rättskällorna. Även om frågan inte är slutligt avgjord finns inte i dagsläget tillräcklig anledning att utgå från att begreppet kan inskränkas på det sätt som eSam föreslagit.

När känsliga personuppgifter som rör hälsa behandlas med stöd av att det är nödvändigt med hänsyn till ett allmänt intresse enligt art. 9(2.h) i GDPR får de bara behandlas av någon, eller under ansvar av någon, som lyder under en legal tystnadsplikt. Eftersom ingen legal tystnadsplikt finns för molntjänstleverantörer är det inte möjligt för myndigheter att outosourca denna typ av personuppgifter i molntjänster i när de behandlas med den nyss nämnda rättsgrunden.

Personuppgifter om lagöverträdelser får bara behandlas under kontroll av myndigheter eller med stöd av legala bestämmelser som fastställer en tillräcklig skyddsnivå. Under kontroll av myndighet ska tolkas så att en personuppgiftsansvarig myndighet kan anlita personuppgiftsbiträden för behandlingen. Det torde därför vara möjligt för myndigheter att anlita molntjänstleverantörer under förutsättning att uppgifterna behandlas med lämplig säkerhet. Den lämpliga säkerheten motsvarar i vart fall den som gäller för känsliga personuppgifter.

8 AVSLUTANDE REFLEKTIONER

I uppsatsen beskrivs många olika faktorer som kan medföra rättsliga hinder för myndigheter att behandla personuppgifter i molntjänster med privata aktörer. Vad avser det legala kravet på en lämplig säkerhetsnivå har personuppgifternas känslighet och informationssystemets risk- och sårbarhet identifierats som de viktigaste faktorerna. Bedömningen av informationssystemets sårbarhet är till stor del en teknisk fråga som kräver fackmässig kunskap inom det området. Frågan om personuppgifternas känslighet är emellertid en juridisk fråga.


Under laglighetsprövningens förlopp kommer bedömningarna av de tekniska frågorna om informationssystemets risk- och sårbarhet mötas med de juridiska bedömningarna av frågorna som rör personuppgifternas känslighet. Vid avgörandet av vilken risk- och sårbarhetsnivå som motsvarar de fastställda kraven på personuppgifternas säkerhetsnivå krävs både teknisk och juridisk kunskap.


De åtgärder som krävs kan dock i sin tur medföra att nytta med molntjänster minskar och att kostnaden för att använda molntjänsterna ökar. När personuppgifterna når en känslighet som överstiger en viss känslighetsnivå kan man därför konstatera att det finns legala hinder för myndigheter att behandla mycket känsliga personuppgifter i molntjänster.

Att en viss leverantör eller tjänst inte lever upp till de rättsliga kraven innebär inte att det föreligger rättsliga hinder för myndigheter att använda molntjänster. Som ovan framgått finns dock många omständigheter som har att göra med molntjänsternas egenskaper som affärsmodell vilka försvårar leverantörernas möjligheter att erbjuda en lämplig molntjänst.

Flera nyckelfrågor i sekretesslagstiftningen som kan medföra legala hinder för myndigheter att lämna ut sekretessreglerade personuppgifter till molntjänstleverantören har behandlats. Först och främst konstaterades att många personuppgifter berörs när en myndighet planerar en outsourcing av personuppgiftsbehandlingen i molntjänster varför prövningen av utlämnande i princip måste göras inom ramen för ett schabloniserat sekretessprövningsförfarande.

Vid bedömningen av skaderisken har många faktorer betydelse, bland annat hur många personer som kommer ta del av uppgifterna, vilka dessa personer är och var de finns. Många av molntjänsternas karakteristiska egenskaper försvårar denna prövning. Om molntjänstleverantören har ett stort antal anställda, underleverantörer eller servrar blir en schabloniserad prövning i praktiken ogenomförbar eftersom den måste göras mot alla som kan komma att ha möjlighet att ta del av uppgifterna. Redan svårigheterna att genomföra prövningen kan sålunda innebära legala hinder avseende utlämnande av personuppgifter till molntjänstleverantörer. Var gränsen går för vilka prövnings som är möjliga att genomföra är en bedömningsfråga som myndigheterna måste ta ställning till i det en-skilda fallet.

Uppsatsen behandlar frågorna om detta hinder kan kringgås genom att överlämnandet av uppgifterna skulle ske med förbehåll om tystnadsplikt, genom att det skulle ske utan att uppgifterna röjs eller genom att det skulle ske med anledning av att ett utlämnande vore nödvändigt för fullgörandet av myndighetens verksamhet.

I uppsatsen konstateras att höga krav föreligger för att en myndighet ska kunna belägga en mottagare med straffsanktionerad tystnadsplikt i utbyte mot information. Denna möjlighet kan inte användas mot molntjänstleverantörer eftersom sådana tystnadsplikter bara får ske avseende viss information och om det är nödvändigt för att skada inte ska uppstå.

Eftersom aktörerna bakom eSam är de myndigheter som är föremål för regleringen har det stor praktisk betydelse vad eSam har för rättsuppfattning i dessa frågor. Av denna anledning har eSams inställning ägnats särskilt intresse i uppsatsen. eSams påstående att utlämnande till molntjänstleverantörer kan vara den enda realistiska lösningen i praktiken för att myndigheter ska kunna fullgöra sin verksamhet har behandlats ingående. Vid utredningen kunde konstaterats att rättskällorna inte ger stöd för att myndigheter kan lämna ut sekretessreglerade uppgifter till molntjänstleverantörer med stöd av den grunden mer än i mycket begränsat utsträckning.

eSam har även uttryckt att endast den anledningen att uppgifterna är tekniskt tillgängliggjorda inte innebär att de röjs. eSam hävdar att uppgifterna inte röjs så länge molntjänstleverantören enligt avtal inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är osannolikt att så sker. Den juridiska argumentationen bakom eSams rättsuppfattning analyseras och kritiseras eftersom den inte enbart verkar bestå av en tolkning av de traditionella rättskällorna.
Eftersom innebörden av begreppet röjande inte är avgjort kan dock inget generellt uttalande om dess innebörder i det aktuella avseendet göras. Generellt gäller dock att förvaltningsmyndigheter bör tolka lagen så att den inte i onödig utsträckning inskränker enskildas rättigheter, varför en tolkning som inskränker begreppet utan tydligt stöd bör undvikas.

De legala kraven som ställs på vilka personuppgifter som myndigheter får outsourca för behandling i molntjänster tar utgångspunkt i personuppgifternas känslighet vad avser både kravet på lämplig säkerhetsnivå och sekretess. Som ovan redovisats uppställs inga legala hinder som medför att personuppgifter med låg känslighet inte kan användas för behandling i molntjänster.

Om myndigheter outsourcar behandling av personuppgifter med högre känslighet innebär det att kraven på molntjänstleverantörens verksamhet stiger. De krav som ställs står ofta i direkt konflikt med de egenskaper hos affärsmodellen molntjänster som medför vinster i förhållande till annan typ av outsourcing. Det framgår av analysen att de åtgärder som krävs av en molntjänstleverantör som ska behandla personuppgifter av känsligare natur medför ökade kostnader samtidigt som nytta minskar. Av den anledningen kan slutsatsen dras att myndigheter drar störst fördel av molntjänster när de använder för personuppgifter som inte är av känslig natur. Samtidigt kan konstateras att fördelarna som dras när personuppgifter av känsligare natur behandlas inte är lika stora.

Det finns en gråzon i frågan om när myndigheter kan använda privata molntjänster för personuppgiftsbehandling. Gråzonen rör emellertid bara de uppgifter som är av känslig natur. Inga legala hinder uppställs för personuppgifter som inte är känsliga. För att myndigheter inte ska riskera lagöverträdelser bör de dock hålla en viss marginal vid bedömningen av om de kan använda en molntjänst i ett visst fall. Ytterligare en anledning till att myndigheter bör ha en konservativ hållning i sina bedömningar är att frågan är politiskt laddad. I de situationer då bedömningen är svår bör myndigheterna därför avvaka ledning från lagstiftaren.

Från politiskt håll har man redan insett att molntjänster har potential att tillföra en effektivisering av den offentliga förvaltningen. I spåren av skandalen hos Transportstyren sedan sommaren år 2017, som så kallade IT-skandalen, har dock debatten rörande vilka risker myndigheters outsourcing av IT-drift kan medföra intensifierats. I väntan på att lagstiftaren utreder frågan och överväger en balans mellan de intressen som aktualiseras bör myndigheterna förhålla sig försiktiga inför att sourcing personuppgifter av känslig karaktär för behandling i molntjänster.

Enkäten från Pensionsmyndigheten visar att informationssäkerhetsarbetet bland myndigheterna behöver förbättras. Att vi går i väntans tider avseende ny lagstiftning innebär sålunda inte att det finns anledning att förhålla sig passiv i frågan om molntjänster inom den offentliga förvaltningen. Enkäten tyder på att de höga krav som ställs när personuppgifter av känslig karaktär behandlas i molntjänster inte alltid efterlevs. Det torde om inte minst den anledningen finnas goda skäl att från politiskt håll intensifiera satsningarna för att vägleda myndigheterna i deras arbete med informationssäkerheten och möjligheterna till att anlita molntjänstleverantörer för personuppgiftsbehandling.
Källförteckning

Litteratur

Magnusson Sjöberg, Cecilia (red.), Andersson, Helena, Edvardsson, Tobias, Johnsson, Sören, Gustaf, Klamborg, Mark, Malmgren, Staffan, Nordbeck, Peter, Nordén, Anna, Jerker B. Svantesson, Dan & Öman, Sören, Rättsinformatik – Juridiken i det digitala informationssamhället, uppl. 2, Studentlitteratur AB, Lund, 2016 [cit. Magnusson Sjöberg m.fl.].


Lindberg, Agne, Kahn, Johan & Krouthén, Björn, IT-Avtal - särskilt om outsourcing – en praktisk handledning, uppl. 1, Norstedts Juridik AB, Stockholm, 2009 [cit. Lindberg m.fl.].


Korling, Fredric & Zamboni, Mauro (red), Juridisk metodlära, uppl. 1, Studentlitteratur AB, Lund, 2013 [cit. Korling & Zamboni].


Sandgren, Claes, Rättssvetenskap för uppsatsförfattare – ämne, material, metod och argumentation, uppl. 3, Norstedts Juridik AB, Stockholm, 2016 [cit. Sandgren].

Bohlin, Alf, Offentlighetsprincipen, uppl. 9, Norstedts Juridik AB, Stockholm, 2015 [cit. Bohlin].

Elektroniskt material

Lydelsen av alla elektroniska länkar kontrollerades den 4 mars 2018.


Europeiska datatillsynsmannen, About, ”https://edps.europa.eu/about-edps_en”.

Europeiska datatillsynsmannen, Glossary, ” https://edps.europa.eu/node/3098#cloudcomputing”.

Magnusson Sjöberg, Cecilia, Personuppgiftslag (1998:204), Lexino, 1 juli 2017 [cit. Sjöberg, Lexino].


Öman, Sören, Lindblom, Hans-Olof, Personuppgiftslagen, En kommentar, uppl. 4 med tillägg och ändringar per v. september 2017, Norstedts Juridik AB, Stockholm, den 16 februari 2018 [cit. Öman & Lindblom].


**Övrig litteratur**

Dataföreningens nätverk Cloud Sweden, *Molnet i offentliga sektorn*, v. 3, 2013 (SW35411/12) [cit. Cloud Sweden, Molnet i offentliga sektorn].


**Offentligt tryck**

*Statens offentliga utredningar*


SOU 2015:39, Slutbetänkande av Informationshanteringsutredningen, Myndighetsdatalag.


*Departementsserien*

Ds 2017:33, Anpassningar till dataskyddsförordningen av registerförfattningar inom Arbetsmarknadsdepartementets ansvarsområde.

*Propositioner*


Prop. 2017/18:95, Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning.

Prop. 2009/10:80, En reformerad grundlag.

Prop. 1979/80:2, med förslag till sekretesslag m.m.

*Utskottsbetänkanden*

KU 1973:26, Konstitutionsutskottets betänkande med anledning av propositionen 1973:90 med förslag till ny regeringsform och ny riksdagsordning m. m. jämte motioner.

*Kommittédirektiv*

Dir. 2011:86, Integritet, effektivitet och öppenhet i en modern e-förvaltning.

Dir. 2014:31, Tilläggsdirektiv till Informationshanteringsutredningen.

Dir. 2009:19, Delegation för e-förvaltning.

*Rättsfall och myndighetsbeslut*

Kammarrätten i Stockholms dom den 30 mars 2005 i mål nr. 1872-04
NJA 1991 s. 103.

JO 2014, dnr 3032-2011.

JO 1994/95 s. 574, dnr 2079-93

JO 1992/93 s. 197, dnr 145-90


**Myndighetspublikationer**

Datainspektionens allmänna råd, *Säkerhet för personuppgifter*, Reviderad november 2008 [cit. DI:s allmänna råd, säkerhet för personuppgifter].

Myndigheten för samhällsskydd och beredskap, Vägledning – Informationssäkerhet i upphandling av system, outsourcing och molntjänster, april 2013 [cit. MSB:s vägledning om informationssäkerhet].


**EU-rättsligt material**

**Fördrag**

Fördraget om Europeiska unionens funktionssätt, 2007 [cit. FEUF].

Fördraget om Europeiska unionen, 2007 [cit. FEU].

Europeiska unionens stadga om de grundläggande rättigheterna, 2007 [cit. Rättighetsstadgan].

**Direktiv och förordningar**

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 [cit. Dataskyddsdirektivet].

Europaparlamentets och rådets förordning (Europeiska unionen) nr 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG [cit. GDPR].

**EU-domstolen**

Mål 6/64 Costa mot ENEL, REG 1964, s. 585, v. 1.

**Europarättsliga myndighetspublikationer**

Arbetsgruppen för skydd av personuppgifter instiftad genom artikel 29 i 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, Yttrande 1/2010 om begreppen registeransvarig och registerförare [cit. WP29, yttrande 1/2010]

Europeiska unionens byrå för nät- och informationssäkerhet, Guidelines for SMEs on the security of personal data processing, December 2016 [cit. ENISA, Guidelines].


Internationella konventioner

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, SÖ 1952:35 [cit. EKMR].

Förenta nationernas deklaration om de mänskliga rättigheterna av den 10 december 1948


Övrigt material


National Institute of Standards and Technology, Recommendations, U.S. department of commerce, Special Publication s. 800-145, September 2011 [NIST].


E-samverkansprogrammet, Outsourcing – en vägledning om sekretess och persondata skydd, januari 2016 [cit. eSams vägledning om sekretess].

