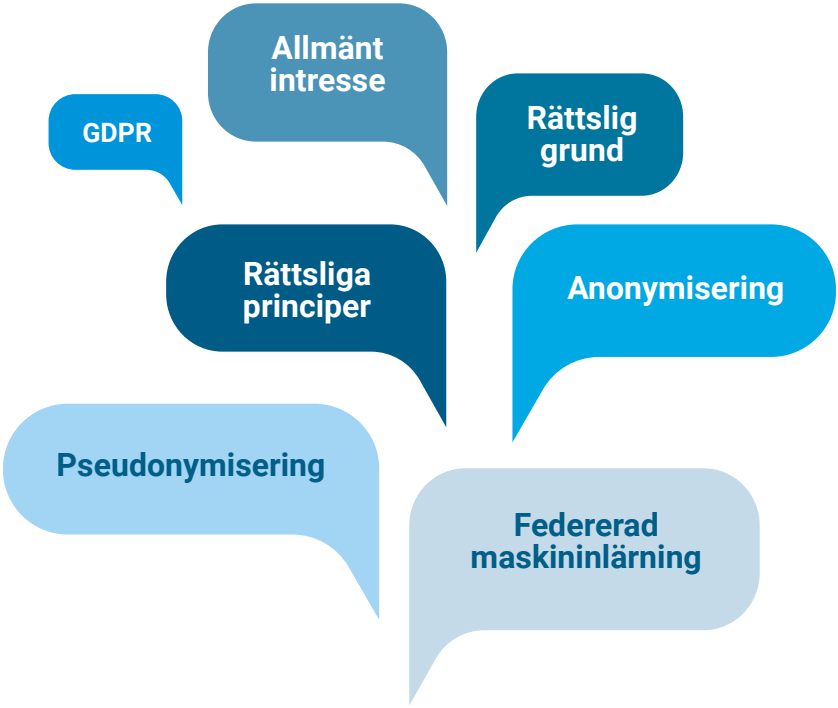
Delning av invånardata från ett juridiskt perspektiv

Jonas Ledendal


Allmänt intresse
GDPR
Rättslig grund
Rättsliga principer
Anonymisering
Pseudonymisering
Federerad maskininlärning

Abstract

Syftet med Datalabbet, som var ett av fem hypoteslabb i projektet ”Den (ut)forskande staden”, var att genom avancerad analys av data, bland annat maskininlärning, bättre kunna förstå kommuninvånarnas komplexa behov och ta fram värdeskapande offentliga tjänster, som kan tillgodose dessa behov och öka invånarnas livskvalitet. För att nå målet var vår hypotes att det krävs analys av stora datamängder och samverkan mellan olika förvaltningar för att få en helhetsbild av de aktuella behoven. Undersökningen har genomförts under åren 2020–2022 i nära samverkan mellan Lunds universitet, Malmö universitet och de olika förvaltningarna i Helsingborgs stad.

Undersökningsmässigt har Datalabbet bestått av två delar: en del som undersökt förutsättningarna för delning av data mellan stadens olika förvaltningar och bolag från ett användarperspektiv (detta behandlas i kapitel 7) och en del som undersökt dessa förutsättningar ur ett juridiskt perspektiv. I det här kapitlet presenteras det juridiska perspektivet. Undersökningen har bland annat innefattat en analys av vilka metoder som kan användas för att anonymisera personuppgifter, vem som ansvarar för behandlingen och vilka krav som ställs för att en myndighets delning av invånardata ska överensstämma med EU:s allmänna dataskyddsförordning (GDPR) och kompletterande nationell dataskyddslagstiftning.


Excel
Greg Harvey
Acrobat
Power Pivot
Search
Notes
Protect Sheet
Protect Workbook
Allow Edit Ranges
Unshare Workbook
Hide ink
Edit Note
Previous Note
Next Note
Show/Hide Note
Show All Notes
Convert to Comments
Jun
Qtr 2
$74,536 $81,990 $90,189 $246,714
27,381 30,119 33,131 $90,632
175,273 192,800 212,080 $580,153
125,744 138,318 152,150 $416,211
168,690 185,559 204,114 $558,363
$571,623 $628,786 $691,664 $1,892,073
13,292 14,597 15,911 43,900
8,477 9,240 10,072 27,789
85,269 92,943 101,308 279,519
82,839 90,295 98,421 271,555
93,649 102,077 111,264 306,990
SVERIGES RIKES LAG
RUS
Artificial Intelligence
A Modern Approach
AR
SCH
DATA & GOLIAT
BRUCE SCHNEIER
TRU
TRUSTED DATA

Rättsliga ramar för delning av data mellan myndigheter

För att kommunala myndigheter ska kunna utföra sina uppdrag, såsom att tillhandahålla välfärdstjänster, meddela tillstånd eller bedriva tillsyn, måste de samla in, bearbeta och lagra data om kommuninvånare. Det är vanligt att varje förvaltning samlar in dessa data som ett led i dess egen ärendehandläggning eller den faktiska verksamhet som myndigheten bedriver. Datainsamling i den kommunala förvaltningen styrs ofta av verksamhetens egna behov och är inte sällan kopplad till handläggningen av ett enskilt ärende. Det är vanligt att data samlas in direkt från kommuninvånaren, exempelvis elevers svar på ett prov eller formulär för ansökan om försörjningsstöd. Förvaltningens digitalisering har dock gjort att sådana uppgifter i allt större utsträckning också samlas in från tredje part, vilket inkluderar andra kommunala och statliga myndigheter, men även kommunala bolag och olika privata aktörer. Ett exempel på det senare är att huvudmannen för en fristående gymnasieskola enligt skollagen ska lämna över en elevs slutbetyg till den kommun där skolan är belägen.[1] Det kan dock även röra sig om en informationstjänst som tillhandahålls av en privat aktör genom avtal med kommunen.

I den här studien har vi fokuserat på delning av data som rör kommuninvånare, det vill säga när en kommunal myndighet samlar in sådana uppgifter från tredje part. De rättsliga ramarna och därmed de rättsliga förutsättningarna för att överföra data ser olika ut beroende på vem som lämnar ut eller tar emot dessa uppgifter. Om ett privaträttsligt subjekt, såsom ett bolag eller en förening, begär att få ta del av uppgifter som förvaras hos en myndighet eller ett kommunalt bolag kan de senare ha skyldighet att göra uppgifterna tillgängliga enligt bestämmelserna om allmänna handlingars offentlighet i tryckfrihetsförordningen (TF).[2] En sådan grundlagsfäst rättighet har inte andra myndigheter, men myndigheter har en på förvaltningslagen (FL) grundad skyldighet att samverka med varandra (8 § FL).[3] Medan handlingsoffentligheten grundas på allmänhetens behov av insyn i den offentliga förvaltningen är samverkansskyldigheten främst grundad på behovet av en effektiv förvaltning. Samverkan ska säkerställa att myndigheterna inte bara ser till sina egna uppgifter utan arbetar för det övergripande målet att skapa goda levnadsvillkor för medborgarna (Prop. 2016/17:180).

Samverkansskyldigheten, så som den kommit till uttryck i förvaltningslagen, utgör också en del av myndighetens serviceskyldighet gentemot enskilda. En myndighet ska nämligen åtminstone i rimlig utsträckning hjälpa den enskilde genom att själv inhämta upplysningar från andra myndigheter (8 § andra stycket FL). En särskild bestämmelse som reglerar en myndighets skyldighet att lämna

1 29 kap. 18 § skollagen (2010:800).
2 När data ska användas för andra ändamål än det ursprungliga ändamål för vilket uppgifterna behandlas av en myndighet kan även lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen bli tillämplig. Det EU-direktiv som lagen genomför har omarbetats (direktiv 2019/1024), och förslag till en ny lag om den offentliga sektorns tillgängliggörande av data har den 7 april 2022 överlämnats till riksdagen (Prop. 2021/22:225). Lagen förväntas träda i kraft i augusti 2022.
3 Förvaltningslagen (2017:900).

ut uppgifter till en annan myndighet finns i 6 kap. 5 § offentlighets- och sekretesslagen (OSL).[4] Även om samverkan mellan myndigheter mycket väl kan ske på frivillig basis, är samverkansskyldigheten en viktig utgångspunkt vid delning av data mellan myndigheter. Om utlämnandet grundas på en skyldighet eller om det sker frivilligt har, som diskuteras nedan, bland annat betydelse vid bedömningen av om eventuella personuppgifter har överförts i enlighet med bestämmelser om dataskydd. Samverkansskyldigheten som sådan utgör dock inte en uppgiftsskyldighet som bryter sekretessen mellan myndigheter (Lundmark & Säfsten 2020). Ett utlämnande måste alltså fortfarande ske i överensstämmelse med bestämmelserna om dataskydd och sekretess.

Rätten till privatliv och rätten till skydd av personuppgifter är grundläggande rättigheter. Artiklarna 7 och 8 i EU:s stadga om grundläggande rättigheter (EU-stadgan) anger att var och en har rätt till respekt för sitt privat- och familjeliv samt rätt till skydd av sina personuppgifter.[5] Sekundärrättsliga bestämmelser som genomför dessa rättigheter finns i EU:s allmänna dataskyddsförordning (GDPR).[6] Ett skydd för den personliga integriteten finns även i den svenska grundlagen. När myndigheter delar data skyddas den personliga integriteten främst av bestämmelserna om sekretess i OSL. Det är dock värt att lägga märke till att EU-rätten har företräde framför nationell rätt, vilket även gäller grundlagen. I *Adidas*-målet åsidosatte EU-domstolen en svensk sekretessbestämmelse som stred mot unionsrätten.[7] Även om medlemsstaterna har större frihet när det gäller att reglera behandling av personuppgifter inom den offentliga sektorn, måste sådan lagstiftning överensstämma med EU-stadgan.

Personuppgifter och anonymisering

Det första en myndighet måste göra när den vill utbyta data med en annan myndighet är att bedöma om den ifrågavarande datamängden innehåller personuppgifter. Med det senare avses enligt artikel 4.1 i GDPR all slags information som rör en nu levande människa (fysisk person). Uppgifter om avlidna eller juridiska personer, såsom bolag, föreningar eller stiftelser, omfattas inte (skäl 14 och 27 GDPR). Personens nationalitet eller bosättningsort saknar däremot betydelse (skäl 14 GDPR). För att förordningen ska bli tillämplig måste den individ som uppgifterna avser (den registrerade) dock antingen vara identifierad eller potentiellt möjlig att identifiera. Det senare innebär att förordningen motsatsvis inte ska tillämpas på anonymiserade uppgifter (skäl 26 GDPR). Om uppgifterna inte redan är anonyma bör myndigheten dels överväga om målet med behandlingen kan uppnås genom att dela anonyma uppgifter, dels bedöma om det finns någon lämplig metod för avidentifiering.

4 Offentlighets- och sekretesslagen (2009:400).
5 Europeiska unionens stadga om de grundläggande rättigheterna, EUT C 326, 26.10.2012, s. 391–407. Se även artikel 8 i Europarådets konvention om skydd för de mänskliga rättigheterna och de grundläggande friheterna.
6 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), EUT L 119, 4.5.2016, s. 1–88.
7 EU-domstolens dom den 14 oktober 1999 i mål C-223/98, *Adidas*, ECLI:EU:C:1999:500.

I sammanhanget är det värt att lägga märke till att pseudonymisering eller kryptering av personuppgifter inte gör dessa anonyma i dataskyddsrättslig mening (skäl 26 GDPR).[8] GDPR kräver ibland att personuppgifter ska pseudonymiseras eller krypteras, men behandlingen omfattas fortfarande av dess andra bestämmelser. Det finns också många tekniska utmaningar vid anonymisering av data. Detta gäller särskilt mot bakgrund av att nya metoder för dataanalys, såsom *big data* och maskininlärning, ökar risken för återidentifiering. I *Breyer*-målet har EU-domstolen slagit fast att personuppgifter ska räknas som anonyma först om risken för identifiering i praktiken är försumbar.[9] Sådan anonymisering kan vara tekniskt svår att genomföra. Artikel 29-gruppen (numera Europeiska dataskyddsstyrelsen) har lämnat vissa rekommendationer om olika avidentifieringsmetoder, men dessa tar inte specifikt upp frågor som rör artificiell intelligens, inklusive maskininlärning.[10] Riktlinjer för anonymisering av personuppgifter håller dock på att utarbetas av Europeiska dataskyddsstyrelsen.

En annan utmaning med anonymisering är att en avvägning måste göras mellan risken för återidentifiering och att bevara uppgifternas användbarhet och kvalitet. Det finns en risk att en sådan gallring leder till ett sämre resultat. En annan teknik som kan användas för att minska riskerna för den registrerade vid samkörning av personuppgifter är federerad maskininlärning. Denna metod bygger på att en algoritm tränas – det vill säga data behandlas – distribuerat över flera klienter (mobila enheter eller servrar) med lokalt lagrade data som inte överförs mellan dessa. En AI-modell kan härigenom tränas på en mycket stor datamängd utan att till exempel personuppgifter eller annan känslig information behöver delas. Tekniken skulle kunna användas av myndigheter som är rättsligt förhindrade att lämna ut personuppgifter.[11] Det kan också vara möjligt att använda syntetiska data, det vill säga data som genererats syntetiskt i stället för att samlas in eller mätas upp. Liksom med traditionell anonymisering finns dock tekniska utmaningar med att generera syntetiska data som håller tillräckligt hög kvalitet.

Ansvarsskyldighet och regelefterlevnad

Det första en myndighet måste göra när den vill utbyta data med en annan myndighet är att bedöma om den ifrågavarande datamängden innehåller personuppgifter samt i vilken utsträckning det är möjligt nå målet med behandlingen genom att i stället använda anonyma uppgifter. När det inte är möjligt, till exempel för att det är tekniskt omöjligt att avidentifiera uppgifterna, får utläm-

8 Artikel 4.5 i förordning (EU) 2016/679 (GDPR) definierar pseudonymisering som ”behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person”.
9 EU-domstolens dom den 19 oktober 2016 i mål C-582/14, *Breyer,* ECLI:EU:C:2016:779.
10 Artikel 29-gruppens yttrande 05/2014 om avidentifieringsmetoder, WP216, antaget den 10 april 2014. Artikel 29-gruppen var en oberoende europeisk arbetsgrupp som behandlade frågor om integritetsskydd och skydd av personuppgifter fram till införandet av GDPR i maj 2018.
11 Federerad maskininlärning är alltså i första hand en lösning på problemet att det finns ett förbud mot att lämna ut uppgifterna (t.ex. på grund av sekretess). Tillgång till personuppgifterna är dock, som konstateras nedan i avsnittet om ansvarsskyldighet, inte en förutsättning för att någon ska anses vara personuppgiftsansvarig. Behandlingen torde alltså i övrigt behöva ske i enlighet med de krav som gäller för skydd av personuppgifter.

nandet och den vidare behandlingen bara utföras om myndigheterna kan uppfylla alla de krav som ställs upp i EU:s dataskyddsförordning. Det senare innefattar att både utlämnandet och den senare behandlingen har en rättslig grund. Om den senare behandlingen är oförenlig med de ändamål för vilka personuppgifterna ursprungligen samlades in måste det enligt principen om ändamålsbegränsning normalt även finnas ett författningsstöd. Den registrerade ska också enligt principen om öppenhet informeras om att hans eller hennes personuppgifter lämnats ut och kommer att behandlas för ett nytt ändamål.

Ansvarsskyldighet

GDPR bygger på principen om ansvarsskyldighet (*accountability*), vilket innebär att det är den personuppgiftsansvarige som har det huvudsakliga ansvaret för att behandling av personuppgifter som denne företar lever upp till de krav som föreskrivs i förordningen (artikel 5.2 GDPR). Det är denne som ska vidta de tekniska och organisatoriska skyddsåtgärder som krävs för att dessa krav ska kunna uppfyllas (artikel 24 GDPR), vilket bland annat innefattar att lämna information till de registrerade och åtgärder som behövs för att behandlingen ska vara säker. Det räcker dock inte att vidta sådana åtgärder, den personuppgiftsansvarige måste också kunna visa att dessa krav faktiskt uppfylls. Om behandlingen inte uppfyller dessa krav kan den personuppgiftsansvarige drabbas av sanktioner (till exempel administrativa sanktionsavgifter). Vem som ska anses vara personuppgiftsansvarig har alltså avgörande betydelse för tillämpningen av förordningen och när ansvar ska utkrävas vid en överträdelse av denna.

Personuppgiftsansvarig är den som bestämmer ändamålen och medlen för behandling av personuppgifter (artikel 4.7 GDPR). Ansvarig är alltså den som utövar ett bestämmande inflytande över behandlingen, men denne måste inte själv utföra behandlingen som sådan. Den som behandlar personuppgifter för någon annans räkning, utan att utöva ett sådant bestämmande inflytande över denna, ska i stället betraktas som personuppgiftsbiträde (artikel 4.8 GDPR). Den senare får endast behandla personuppgifter enligt den personuppgiftsansvariges instruktioner (artikel 29 GDPR), men har även vissa egna skyldigheter enligt GDPR. Det framgår av artiklarna 4.7 och 4.8 i GDPR att en myndighet eller ett annat offentligt organ kan vara både personuppgiftsansvarig och biträde. Exempelvis behandlar Statens servicecenter i stor utsträckning personuppgifter i egenskap av personuppgiftsbiträde för andra myndigheter. Vem som är ansvarig för behandlingen bestäms inom det kommunala specialreglerade området dessutom inte sällan genom lag eller annan författning.[12]

I rättspraxis har kommunstyrelsen och de kommunala nämnderna normalt ansetts vara personuppgiftsansvariga (Öman 2021). Dessa utgör förvisso inte egna juridiska personer men är att betrakta som myndigheter i statsrättslig bemärkelse (Strömberg & Lundell 2018). Det är dock värt att lägga märke till att både Europeiska dataskyddsstyrelsen och Integritetsskyddsmyndigheten (IMY) har

12 Se bl.a. 11 § förordning (2001:637) om behandling av personuppgifter inom socialtjänsten, som anger att en kommunal myndighet är personuppgiftsansvarig för den behandling av personuppgifter inom socialtjänsten som myndigheten utför.

ansett att personuppgiftsansvarsbegreppet ska tolkas funktionellt, det vill säga att det avgörande är vem som faktiskt beslutat om ändamålen och medlen, inte vem som haft den formella befogenheten att fatta ett sådant beslut.[13] För att fastställa vem som ansvarar för behandlingen är det alltså nödvändigt att göra en bedömning av de faktiska omständigheterna i det enskilda fallet. Det är här värt att uppmärksamma att varken behandlingens ändamål eller väsentliga beslut om medlen för densamma kan överlåtas till någon annan, till exempel en leverantör, utan att detta påverkar ansvarsfördelningen.

När det gäller delning av personuppgifter måste en bedömning göras av om det finns ett gemensamt ändamål. Det framgår nämligen av artikel 26 i GDPR att om fler än en organisation varit med och bestämt ändamålen och medlen så uppkommer gemensamt personuppgiftsansvar. Detta begrepp har de senaste åren genom EU-domstolens praxis fått en mer vidsträckt innebörd. I *Wirtschaftsakademie*-målet slog domstolen fast att gemensamt ansvar kan uppkomma även om samtliga ansvariga inte haft tillgång till personuppgifterna.[14] Detta vidareutvecklades i *Fashion ID*-målet där domstolen förtydligade att gemensamt ansvar dock inte nödvändigtvis innebär att alla som deltagit i behandlingen har ett lika långtgående ansvar.[15] När gemensamt ansvar föreligger ankommer det på de personuppgiftsansvariga att upprätta ett inbördes arrangemang, som under öppna former bland annat fastställer deras inbördes ansvar (artikel 26 GDPR). Arrangemangets form regleras inte i förordningen, men enligt Europeiska dataskyddsstyrelsens riktlinjer om personuppgiftsansvar bör detta fastställas i ett avtal eller någon annan bindande rättsakt. Att personuppgiftsansvar inte sällan är författningsreglerat inom det kommunala området gör dessutom frågan om gemensamt ansvar vid delning av invånardata särskilt komplicerad.[16]

Laglighet – rättslig grund

För att behandling av personuppgifter ska vara laglig måste den ha en rättslig grund (artikel 5.1 a GDPR). Om behandlingen saknar rättslig grund är den otillåten. Vad som kan utgöra rättslig grund anges i artikel 6.1 i GDPR. Den uppräkning av grunder som görs i denna bestämmelse är uttömmande och av *ASNEF*-målet framgår att en medlemsstat varken kan införa nya rättsgrunder eller utvidga deras tillämpningsområde.[17] Detta innebär att den personuppgiftsansvarige måste kunna grunda behandlingen på antingen den registrerades samtycke eller någon av de andra grunder som räknas upp i artikel 6.1. För myndigheter gäller dock vissa begränsningar. Dessa kan normalt varken använda samtycke (artikel 6.1 a GDPR) eller den så kallade intresseavvägningsregeln (artikel 6.1 f GDPR), som vanligtvis används inom den privata sektorn.[18] Att striktare regler gäller för

13 Europeiska dataskyddsstyrelsens riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, antagna den 7 juli 2021.
14 EU-domstolens dom den 5 juni 2018 i mål C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388.
15 EU-domstolens dom den 29 juli 2019 i mål C-40/17, *Fashion ID*, ECLI:EU:C:2019:629.
16 Se dock. 11 § förordning (2001:637) om behandling av personuppgifter inom socialtjänsten, som anger att om behandlingen görs gemensamt för flera myndigheter inom kommunen är varje myndighet personuppgiftsansvarig för den behandling som utförs hos den myndigheten.
17 EU-domstolens dom den 24 november 2011, *ASNEF*, ECLI:EU:C:2011:777.
18 Ett visst utrymme att använda samtycke eller intresseavvägningsregeln även inom den offentliga förvaltningen synes finnas enligt utta-

offentlig sektor har bland annat motiverats med att den registrerade ofta har en skyldighet att lämna uppgifter till en myndighet (Blume 2015).

> ***Att striktare regler gäller för offentlig sektor har bland annat motiverats med att den registrerade ofta har en skyldighet att lämna uppgifter till en myndighet.***

För myndigheter innebär det att behandlingen normalt måste grundas på en rättslig förpliktelse (artikel 6.1 c GDPR) eller uppgift av allmänt intresse eller myndighetsutövning (artikel 6.1 e GDPR). För delar av den kommunala verksamheten kan det även bli aktuellt att grunda behandling på avtal (artikel 6.1 b GDPR), men detta är endast möjligt när behandlingen är nödvändig för att ingå eller fullgöra ett avtal mellan myndigheten och den registrerade, vilket gör att även denna grund har ett begränsat tillämpningsområde. Artikel 6.1 c i GDPR ska dessutom tolkas restriktivt och förutsätter att myndigheten inte har någon valfrihet. Oavsett om behandlingen grundas på artikel 6.1 c eller e måste skyldigheten eller uppgiften föreskrivas i lag eller annan författning. Myndigheten måste också kunna visa att behandlingen är nödvändig, det vill säga att samma mål inte kan uppnås genom mindre ingripande åtgärder. Exempelvis när det räcker med anonyma uppgifter.[19]

För centrala delar av den kommunala verksamheten gäller dessutom speciallagstiftning som närmare anger under vilka förhållanden det är tillåtet att behandla personuppgifter. För vissa områden har den svenska lagstiftaren valt att göra en uttömmande reglering av för vilka ändamål uppgifterna får behandlas. Exempelvis lagen om behandling av personuppgifter inom socialtjänsten.[20] Datainspektionen (numera IMY) har bland annat konstaterat att rättslig grund för samkörning därför saknades när ett landsting och en kommunal nämnd (vård- och omsorgsnämnden) överfört personuppgifter för gemensam verksamhetsuppföljning.[21] Eftersom samkörningen inte var nödvändig för utförande av en uppgift inom socialtjänsten saknades stöd för behandlingen i den nämnda lagen. Det finns dock även områden där sådan detaljerad speciallagstiftning inte förekommer, exempelvis det skollagsreglerade området. Sådana skillnader kan skapa hinder för samverkan mellan myndigheter.

landen av Europeiska dataskyddsstyrelsen (riktlinjer 5/2020, punkt 16-20) och Artikel 29-gruppen (yttrande 6/2014 s. 22-23). Det torde dock primärt röra sig om uppgifter som ligger utanför myndighetens kärnverksamhet.
19 EU-domstolens dom den 16 december 2008 i mål C-524/06, Huber, ECLI:EU:C:2008:724.
20 Lagen (2001:454) om behandling av personuppgifter inom socialtjänsten.
21 Datainspektionens beslut 2015-07-03, dnr 518-2015 och 643-2015.

Det är samtidigt viktigt att uppmärksamma att myndigheter inte sällan behandlar känsliga personuppgifter. Sådana uppgifter är det förbjudet att behandla om den registrerade inte har lämnat ett uttryckligt samtycke eller om behandlingen kan stödjas på något av de andra undantag som anges i artikel 9 i GDPR. För myndigheter innebär det att behandlingen normalt ska ha stöd i lag. Att det finns specialreglering kan alltså vara en förutsättning för att till exempel socialtjänsten ska kunna bedriva sin verksamhet. Det är också värt att lägga märke till att de kompletterande bestämmelser som finns i skollagen i huvudsak gäller känsliga personuppgifter.[22] Exempelvis är det vanligtvis nödvändigt att behandla sådana uppgifter i samband med en frånvaroutredning eller beslut om särskilt stöd. Även för behandling av person- eller samordningsnummer gäller striktare regler, som begränsar när dessa kan lämnas ut till en annan myndighet vid samkörning av personuppgifter.[23]

Korrekthet

Förutom principen om laglighet ställs i artikel 5.1 a i GDPR även krav på att behandlingen ska vara korrekt. Det är alltså inte tillräckligt att behandlingen är laglig. Vad som avses med kravet på korrekthet (*fairness*) är inte helt klart, men det uppfattas ofta som ett allmänt krav på att behandlingen inte ska vara otillbörlig (Holtz & Ledendal 2020). Med utgångspunkt från de uttalanden som görs i ingressen till GDPR är det tänkbart att lagstiftarens avsikt varit att principen ska tolkas i ljuset av unionens rättsliga ram för otillbörliga affärsmetoder, det vill säga att den tar sikte på metoder som starkt avviker från god affärssed, strider mot tro och heder eller som kännetecknas av en avsevärd obalans mellan rättigheter och skyldigheter. Principen skulle då få särskild betydelse vid behandling som grundas på samtycke (artikel 6.1 a GDPR). Det är dock värt att lägga märke till att detta krav även gäller för myndigheter.

Av Integritetsskyddsmyndighetens praxis följer att en myndighets behandling av personuppgifter kan vara otillåten om den sker på ett sätt som strider mot principen om korrekthet. IMY har bland annat ansett att en kommuns kamerabevakning av en boendes sovrum på ett LSS-boende var så ingripande att den inte levt upp till kravet på korrekthet i dataskyddsförordningen (beslut 2020-11-24, dnr. DI-2019-7782). Bevakningen saknade dock även rättslig grund. I ett senare tillsynsärende har IMY emellertid funnit att kamerabevakning av brandstation som skedde på anställdas plats för ombyte vid larm stred mot principen om korrekthet trots att den personuppgiftsansvarige ansetts ha rättslig grund för behandlingen enligt lagen om skydd mot olyckor (beslut 2021-06-09, dnr. DI-2018-22697). Av beslutet framgår att myndigheten betraktar principerna om laglighet och korrekthet som två separata krav samt att den senare förutsätter att det görs en intresseavvägning för att fastställa om behandlingen är oskälig i förhållande till den registrerade.[24]

22 26 a kap. 4–5 §§ skollagen (2010:800).
23 Artikel 87 i förordning (EU) 2016/679 (GDPR) anger att medlemsstaterna närmare får ange under vilka villkor nationella identifikationsnummer får behandlas. I 3 kap. 11–12 §§ lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning anges att sådana nummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.
24 Stöd för detta synsätt har IMY hämtat i förarbetena till dataskyddslagen (prop. 2017/18:105 s. 47) och dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd.

Ändamålsbegränsning

Principen om ändamålsbegränsning anger att den personuppgiftsansvarige innan personuppgifter samlas in alltid måste fastställa behandlingens syfte (artikel 5.1 b GDPR). Detta ändamål måste dessutom vara berättigat. Uppgifterna får samlas in för fler än ett syfte, men vart och ett av dessa syften måste kunna specificeras på ett tydligt sätt. När uppgifterna väl har samlats in får de inte behandlas på något sätt som är oförenligt med dessa ändamål. När personuppgifter lämnas ut till en annan myndighet måste en bedömning alltså göras om det rör sig om ett nytt ändamål. För det fall uppgifterna har samlats in för det aktuella ändamålet kan utlämnandet stödjas på samma rättsliga grund (skäl 50). Om detta inte är fallet är det nödvändigt att bedöma om utlämnandet och den vidare behandlingen är förenliga med det ursprungliga ändamålet. Hur denna bedömning ska göras anges i artikel 6.4 i GDPR. När behandlingen är att anse som oförenlig är utlämnandet endast tillåtet med den registrerades samtycke eller med stöd i lag eller annan författning.

För myndigheter innebär ändamålsbegränsningsprincipen att ett utlämnande till en annan myndighet normalt kräver att ändamålet med den vidare behandlingen är förenligt med det ändamål för vilket uppgifterna ursprungligen samlades in. Det följer av artikel 5.1 b i GDPR att så normalt ska vara fallet när uppgifterna behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Det senare förutsätter dock att särskilda skyddsåtgärder har vidtagits enligt artikel 89.1 i GDPR. Exempelvis kan det krävas att uppgifterna pseudonymiserats. När det nya ändamålet är oförenligt krävs däremot normalt lagstöd. Högsta förvaltningsdomstolen (HFD) har ansett att bestämmelserna om uppgiftsskyldighet mellan myndigheter i 6 kap. 5 § OSL gör att någon prövning enligt artikel 5.1 b inte ska göras i det enskilda fallet (HFD 2021 ref. 10). Det är dock tveksamt om detta överensstämmer med unionsrätten. Jämför bland annat EU-domstolens dom i *Latvijas*-målet där domstolen slog fast att nationella bestämmelser som sammanjämkar rätten till skydd av personuppgifter med allmänhetens rätt till tillgång till allmänna handlingar måste överensstämma med EU:s stadga om grundläggande rättigheter.[25]

Uppgiftsminimering

Principen om uppgiftsminimering anger att ett utlämnande eller annan behandling av personuppgifter endast får omfatta uppgifter som är adekvata och relevanta i förhållande till ändamålet med behandlingen (artikel 5.1 c GDPR). Det är enligt samma princip inte heller tillåtet att lämna ut eller behandla fler uppgifter än vad som behövs för att uppnå målet med behandlingen. Principen ger uttryck för ett allmänt krav på att behandlingen ska vara nödvändig och proportionerlig. Det är värt att lägga märke till att det från detta krav inte görs något undantag för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Även när personuppgifter behandlas för forskningsändamål måste det alltså göras en bedömning av om målet med behandlingen kan uppnås genom att färre uppgifter behandlas. Principen är inte oför-

25 EU-domstolens dom den 22 juni 2021 i mål C-439/19, *Latvijas Republikas Saeima*, ECLI:EU:C:2021:504.

enlig med behandling av mycket stora datamängder, men även vid maskininlärning, där det kan vara avgörande, måste den personuppgiftsansvarige kunna visa att det är nödvändigt och proportionerligt. Exempelvis kan den ansvarige behöva visa att samma resultat inte kan uppnås genom traditionella statistiska metoder som bygger på ett representativt urval.

Lagringsminimering

Principen om lagringsminimering anger att personuppgifter inte får bevaras under längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas (artikel 5.1 e GDPR). När uppgifterna inte behövs för dessa ändamål ska de raderas eller avidentifieras. Från detta (liksom från principen om ändamålsbegränsning) görs dock undantag för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Principen hindrar alltså inte att myndigheter arkiverar eller bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Det är dock värt att lägga märke till att undantaget förutsätter att särskilda skyddsåtgärder har vidtagits enligt artikel 89.1 i GDPR. Det räcker alltså inte att det i och för sig finns stöd i svensk nationell rätt.

För att uppfylla kravet på lagringsminimering måste en myndighet ange de perioder under vilka uppgifterna kommer att lagras eller åtminstone de kriterier som ska användas för att fastställa dessa perioder. Det är inte helt klart hur artikel 5.1 e i GDPR förhåller sig till den svenska arkivlagstiftningen, som har ett nära samband med offentlighetsprincipen. Högsta förvaltningsdomstolen har dock ansett att arkivlagens bestämmelser om bevarande och gallring inte gav något utrymme för att beakta enskildas intressen av skydd för personlig integritet (HFD 2015 ref. 71). Någon möjlighet för den registrerade att få allmänna handlingar gallrade med stöd av dataskyddsrättslig lagstiftning fanns inte enligt domstolen. Svensk rättspraxis bygger på en föreställning om att medlemsstaterna har en betydande frihet att reglera hur personuppgifter behandlas inom offentlig sektor, men det kan ifrågasättas om detta numera överensstämmer med unionsrätten.[26]

Öppenhet

Personuppgifter ska som utgångspunkt behandlas på ett öppet sätt i förhållande till den registrerade. I det numera upphävda direktiv 95/46/EG (dataskyddsdirektivet) skulle principen om korrekthet även säkerställa den registrerades rätt till insyn i behandlingen genom att förbjuda hemlig insamling och behandling av dennes personuppgifter.[27] Detta säkerställs dock primärt numera av den nya princip om öppenhet som infördes genom dataskyddsförordningen (artikel 5.1 a GDPR). Att det fortsatt finns ett starkt samband mellan de både principerna framgår dock av att dessa på ett antal ställen i förordningen nämns tillsammans. Vad som närmare avses med att personuppgifter ska behandlas på ett öppet och korrekt sätt i förhållande till den registrerade anges i artiklarna 12–15 i

26 Se bland annat ovan vad EU-domstolen uttalat i mål C-439/19 *Latvijas*, som även torde ha relevans för behandling av personuppgifter för arkivändamål av allmänt intresse.
27 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, EGT L 281, 23.11.1995, s. 31–50.

GDPR. Sådan information ska alltid utformas på ett tydligt och klart sätt (artikel 12 GDPR). När den riktar sig till ett barn, såsom i skolan eller kultur och fritid, ska den anpassas till barnets ålder (skäl 58 GDPR). Det är inte tillräckligt att informera vårdnadshavarna.

Det framgår av artiklarna 13 och 14 i GDPR att den registrerade har rätt att få information om till vem dennes personuppgifter lämnas ut. Sådana mottagare eller åtminstone kategorier av mottagare ska både anges i samband med att uppgifterna samlas in från den registrerade (artikel 13.1 e GDPR) och när uppgifterna erhålls från tredje part (artikel 14.1 e GDPR). Att detta även gäller för delning av data mellan myndigheter har slagits fast av EU-domstolen i *Bara*-målet.[28] Vad som avses med ”mottagare” definieras i artikel 4.9 i GDPR. Av definitionen framgår att skyldigheten inte bara omfattar utlämnanden till tredje part, utan även andra mottagare (till exempel personuppgiftsbiträden). Ett undantag görs dock när personuppgifter lämnas ut till en myndighet för att användas vid handläggningen av ett enskilt ärende, exempelvis i samband med ett tillsynsärende, och behandlingen sker med stöd i lag eller annan författning. Den registrerade ska också informeras om att dennes personuppgifter kommer att behandlas för ett annat syfte än för vilket de ursprungligen samlades in (artiklarna 13.3 och 14.4 GDPR). Detta gäller oberoende av om behandlingen enligt artikel 6.4 i GDPR är förenlig eller oförenlig med det ursprungliga syftet.

Från ovanstående informationsskyldighet görs vissa undantag. För information som ska lämnas enligt antingen artikel 13 eller 14 görs undantag när den registrerade redan förfogar över informationen. Det är inte helt klart hur detta ska tolkas. IMY har tidigare gjort en förhållandevis generös tolkning av motsvarande undantag i personuppgiftslagen, men det är inte helt självklart att den tolkningen är relevant i förhållande till de mer detaljerade bestämmelser som finns i GDPR. När det gäller personuppgifter som erhållits från tredje part finns det däremot fler undantag (artikel 14.5 GDPR). Av relevans för utlämnande mellan myndigheter är bland annat att sådan information inte behöver lämnas när utlämnandet är uttryckligen föreskrivet i lag eller annan författning (artikel 14.4 c GDPR). En sådan bestämmelse måste dock fastställa lämpliga skyddsåtgärder. Bestämmelsen måste enligt *Bara*-målet också vara tillräckligt tydlig och ha publicerats i en författningssamling. Det räcker alltså inte att utlämnandet i och för sig har stöd i lag.

Vi har i Datalabbet undersökt möjligheten att minska riskerna för enskilda individer genom att endast dela anonym information, särskilt genom federerad maskininlärning och syntetisering av data.

28 EU-domstolens dom den 1 oktober 2015 i mål C-201/14, *Bara m.fl.*, ECLI:EU:C:2015:638.

Avslutande diskussion

GDPR är i princip tillämplig vid all behandling av personuppgifter, det vill säga data som rör en identifierad eller identifierbar fysisk person (människa). Det första en myndighet måste göra när den vill utbyta data är att bedöma om den ifrågavarande datamängden innehåller personuppgifter. Vi har i Datalabbet undersökt möjligheten att minska riskerna för enskilda individer genom att endast dela anonym information, särskilt genom federerad maskininlärning och syntetisering av data. Det finns dock tekniska utmaningar med alla metoder för avidentifiering. En avvägning måste göras mellan risken för återidentifiering och uppgifternas kvalitet. Rättsläget är delvis oklart, men för att räknas som anonym i dataskyddsrättslig mening ska risken för att en individ direkt eller indirekt kan identifieras eller återidentifieras i praktiken vara försumbar. Pseudonymisering och kryptering är inte tillräckligt. Europeiska dataskyddsstyrelsen håller på att ta fram nya riktlinjer om anonymisering, som förhoppningsvis kan leda till mer klarhet.

Det är den personuppgiftsansvarige som har det huvudsakliga ansvaret för all behandling av personuppgifter som denne själv utför eller som utförs för dennes räkning. Den ansvarige ska enligt principen om ansvarsskyldighet både vidta lämpliga tekniska och organisatoriska skyddsåtgärder och kunna visa att dessa uppfyller de krav som gäller enligt GDPR. Ansvarig för behandling av personuppgifter i kommunal förvaltning är normalt den nämnd (myndighet) som rent faktiskt beslutat om ändamålen och medlen för behandlingen. Vem som är ansvarig i kommunal verksamhet (till exempel inom socialtjänsten) pekas dock inte sällan ut direkt genom lag eller annan författning. När beslutet fattats av fler än en organisation blir de gemensamt ansvariga. Vid delning av data, särskilt när det sker för ett gemensamt syfte, uppkommer normalt ett sådant gemensamt ansvar. När personuppgiftsansvaret slås fast direkt i lag har förekomsten av gemensamt ansvar dock inte alltid beaktats av lagstiftaren, vilket kan leda till att rättsläget blir oklart vid samverkan mellan myndigheter.

Den som behandlar personuppgifter måste alltid ha en rättslig grund. Det följer av Integritetsskyddsmyndighetens praxis att rättslig grund kan saknas när myndigheter samkör personuppgifter. En myndighet kan normalt inte använda samtycke eller den så kallade intresseavvägningsregeln som rättslig grund, vilket innebär att samkörningen måste kunna grundas på en rättslig förpliktelse eller uppgift av allmänt intresse eller myndighetsutövning som har stöd i lag eller annan författning. En kommunal myndighets möjlighet att dela personuppgifter och samköra dessa med en annan myndighet är alltså normalt beroende av hur de särskilda bestämmelser som gäller för myndigheten i fråga har utformats. Av undersökningen har framgått att dessa möjligheter i väsentliga delar skiljer sig åt mellan bland annat den skollagsreglerade verksamheten och socialtjänsten. För att möjliggöra sådan delning av data mellan olika kommunala förvaltningar som är önskvärd för att bland annat förstå kommuninvånarnas komplexa behov och ge ökad service kan det alltså krävas lagändringar. De allmänna bestämmelserna i GDPR medför däremot inte några avsevärda hinder mot sådan delning av data inom offentlig förvaltning förutsatt att behandlingen uppfyller de krav som ställs upp i förordningen.


Artificial Intelligence and Social Work
TAMBE AND RICE
ART
361.3
SVERIGES RIKES LAG
JOHAN MUNCK
2016

Referenser

Artikel 29-gruppens yttrande 05/2014 om avidentifieringsmetoder, WP216, antaget den 10 april 2014.

Artikel 29-gruppens yttrande 06/2014 om begreppet den registeransvariges berättigade intresse enligt artikel 7 i direktiv 95/46/EG, WP217, antaget den 9 april 2014.

Blume (2015). *The Public Sector and the Forthcoming EU Data Protection Regulation*. European Data Protection Law Review. Vol. 1, nr 1, s. 32-38.

Europeiska dataskyddsstyrelsens riktlinjer 04/2019 om artikel 25 Inbyggt dataskydd och dataskydd som standard, antagna den 20 oktober 2020.

Europeiska dataskyddsstyrelsens riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, antagna den 4 maj 2020.

Europeiska dataskyddsstyrelsens riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, antagna den 7 juli 2021.

Holtz & Ledendal (2020). *Överlappningen mellan dataskydd och marknadsrätt – Dataskyddsförordningens tillämpning på marknadsföring och marknadsrättens tillämpning på kommersiell personuppgiftsbehandling.* Svensk juristtidning s. 140.

Lundmark & Säfsten (2020). *Förvaltningslagen – en kommentar*. Norstedts Juridik.

Regeringens proposition 2016/17:180 *En modern och rättssäker förvaltning – ny förvaltningslag*.

Regeringens proposition 2017/18:105 *Ny dataskyddslag*.

Regeringens proposition 2021/22:225 *Den offentliga sektorns tillgängliggörande av data*.

Strömberg & Lundell (2018). *Allmän förvaltningsrätt*. Liber.

Öman (2021). *Dataskyddsförordningen (GDPR) m.m. – en kommentar*. Norstedts Juridik.

Rättsfallsförteckning

Europeiska unionens domstol

Dom den 14 oktober 1999 i mål C-223/98, Adidas, ECLI:EU:C:1999:500.

Dom den 16 december 2008 i mål C-524/06, Huber, ECLI:EU:C:2008:724.

Dom den 24 november 2011, ASNEF, ECLI:EU:C:2011:777.

Dom den 1 oktober 2015 i mål C-201/14, Bara m.fl. ECLI:EU:C:2015:638.

Dom den 19 oktober 2016 i mål C-582/14, Breyer, ECLI:EU:C:2016:779.

Dom den 5 juni 2018 i mål C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388.

Dom den 29 juli 2019 i mål C-40/17, Fashion ID, ECLI:EU:C:2019:629.

Dom den 22 juni 2021 i mål C-439/19, Latvijas Republikas Saeima, ECLI:EU:C:2021:504.

Högsta förvaltningsdomstolen

HFD 2015 ref. 71

HFD 2021 ref. 10

Integritetsskyddsmyndigheten

Beslut 2015-07-03, dnr 518-2015 och 643-2015.

Beslut 2020-11-24, dnr. DI-2019-7782.

Beslut 2021-06-09, dnr. DI-2018-22697

Författarpresentation

Jonas Ledendal är universitetslektor i handelsrätt vid Institutionen för handelsrätt, Ekonomihögskolan vid Lunds universitet. Han forskar om den digitala omvandlingens rättsliga ramar, särskilt med inriktning på öppenhet, sekretess och dataskydd.

Den (ut)forskande staden

Denna rapport är ett utdrag ur antologin *Den (ut)forskande staden – En FoU-innovation i offentlig sektor* (publicerad på fou.helsingborg.se/rapporter).

Den (ut)forskande staden är ett projekt som har drivits av FoU Helsingborg 2019-2022 och har fungerat som en testbädd där stadens förvaltningar, akademi och invånare tillsammans haft möjlighet att skapa och testa nya lösningar på gamla problem. I samverkan har man utforskat nya arbetssätt för utvecklingsarbete för att på så sätt inspirera och påverka omställningen av organisationen mot en större innovativ förmåga.

I *Den (ut)forskande staden – En FoU-innovation i offentlig sektor* får läsaren följa med på de resor som projektets 14 forskare gjort. Dessa omfattar både mer övergripande resor såsom hur en offentlig organisation systematiskt kan arbeta med att lära sig nya - utforskande och samverkande - arbetssätt för innovation, och mer fokuserade resor genom de fem så kallade *hypoteslabben*.