HELSINGBORG

Kommunala myndigheters delning av invånardata

Slutrapport från Datalabbet i Helsingborgs stad

Sara Leckner, Jonas Ledendal och Annika Nilsson

LUNDS UNIVERSITET

MALMÖ UNIVERSITET

Helsingborgs stad
Avdelningen för innovation och transformation
Programstöd Forskning
fou.helsingborg.se
2023

Formgivning: Annika Nilsson
Foto omslag: Axel Victorin

Innehåll

Förkortningar och begrepp

C	Domstolen i domar från EU-domstolen (målnummer)
DI	Datainspektionen (numera Integritetsskyddsmyndigheten)
dnr.	diarienummer
EDPB	European Data Protection Board (Europeiska dataskyddsstyrelsen)
EG	Europeiska gemenskaperna
EU	Europeiska unionen
EUD	Europeiska unionens domstol
FEUF	Fördraget om Europeiska unionens funktionssätt
FL	Förvaltningslag (2017:900)
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG. GDPR benämns också allmänt som dataskyddsförordningen.
HFD	Högsta förvaltningsdomstolen
IMY	Integritetsskyddsmyndigheten (tidigare Datainspektionen)
OSL	Offentlighets- och sekretesslag (2009:400)
Prop.	proposition
ref.	referatmål
SOU	Statens offentliga utredningar
SWOT	Metod för att analysera en organisations, grupps eller process styrkor, svagheter, hot och möjligheter, ofta inför ett pågående eller kommande förändringsarbete eller i relation till förändringar i omgivningen.
T	Tribunalen i domar från EU-domstolen (målnummer)
TF	Tryckfrihetsförordning (1949:105)
WP	Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Artikel 29-gruppen)

Sammanfattning

Datalabbet har drivits i Helsingborgs stad som en del av det stadsövergripande projektet *Den (ut)forskande staden* 2019-2022. Datalabbet genomfördes i samverkan mellan Malmö universitet, Lunds universitet, Digitaliseringsavdelningen i Helsingborgs stad samt FoU Helsingborg.

För att kunna upprätthålla välfärden, och möta de många utmaningar vi står inför, måste den offentliga sektorn hitta nya, effektiva sätt att arbeta. En möjlig väg för att effektivisera den offentliga verksamheten, skulle kunna vara att hitta nya sätt att använda data som kommunen samlar in. I detta projekt har staden velat utforska den outnyttjade potential av kunskap som finns i de data invånarna har delat med sig av till kommunen. Hypotesen är att om data från olika förvaltningar kunde kombineras och analyseras på nya relevanta sätt, oberoende av förvaltningsgränserna, skulle man få en mer komplett förståelse för invånarnas situation och på så sätt kunna erbjuda bättre service och tjänster. En sådan samordning av data skulle dock innebära en ny form av intrång i kommuninvånarnas integritet och det är inte säkert att invånarna förstår eller vill ge sitt samtycke till det. Det är också oklart vad förvaltningarna och kommunen som helhet juridiskt får göra när det kommer till datadelning. Delning av invånardata väcker med andra ord både etiska (vad *bör* man göra?) och rättsliga frågor (vad *får* man göra?). I Datalabbet har vi velat utforska båda dessa frågor och sätta dem i relation till varandra.

Sara Leckners delstudie har ett etiskt perspektiv, och syftar till att fånga medborgarnas inställning till kommunens nuvarande och önskade dataanvändning. Målet är att ge underlag till hur datadriven teknik kan användas på ett etiskt sätt, utifrån invånarnas perspektiv. De metoder som använts är bland annat enkäter och fokusgrupper. Resultaten presenteras i form av en SWOT-analys. SWOT-analysen visar att invånarna i Helsingborgs stad har stor tillit till kommunens sätt att hantera data. Tilliten bygger på att kommunen måste följa ett strikt regelverk och vara transparenta med hur data samlas in och används. Invånarna upplever därför att de har kontroll över hur den data de lämnar till kommunen används. Denna tillit är viktig att förvalta. Det framkommer också att invånarna i nuläget förutsätter att kommunen redan samkör data. Därmed tycks inte samkörning som sådan vara något problem, förutsatt att regelverket efterföljs. Det innebär att invånarna lägger över en stor del av kontrollen av sin integritet på kommunen, vilket ytterligare talar för att kommunen behöver involvera invånarna i sin digitalisering av tjänster och motivera dem att mer aktivt agera och ta kontroll över sin integritet.

Jonas Ledendals delstudie utgår från ett juridiskt perspektiv och syftar till att undersöka de rättsliga förutsättningarna för att dela data mellan kommunala myndigheter. I delstudien undersöks också om de bestämmelser som gäller för kommunala myndigheter, utgör särskilda hinder för att tillhandahålla digitala tjänster till invånarna i den egna kommunen. Denna delstudie utgår från det som brukar kallas traditionell rättsvetenskaplig metod. Resultatet visar att eftersom insamling och utlämnande av personuppgifter i sig utgör en behandling av personuppgifter, måste även de uppfylla de grundläggande principer för dataskydd som slås fast i EU:s dataskyddsförordning. Vid

varje datainsamling behöver ändamålet med behandlingen och en rättslig grund bestämmas. För myndigheter finns en begränsad möjlighet att använda samtycke eller den så kallade intresseavvägningsregeln som rättslig grund, vilket innebär att behandlingen normalt måste grunda sig på en rättslig förpliktelse eller en uppgift av allmänt intresse som har fastställts i lag eller annan författning. Detta lämnar med nuvarande reglering ett begränsat utrymme för att dela data mellan förvaltningar, till exempel för gemensamma utvärderingar. Jonas Ledendal fördjupar sig vidare i anonymiserade data, syntetisk data och federerad maskininläsning som alternativa vägar, men konstaterar att det finns få helt säkra metoder för att dela uppgifter mellan myndigheter.

Rapporten avslutas med en gemensam diskussion där ett antal skärningspunkter mellan det etiska och det juridiska perspektivet lyfts fram. En viktig slutsats från projektet är att de hinder som finns för att dela eller samköra data för att på ett bättre sätt utföra de uppgifter som åligger kommunen inte sällan beror på att den svenska lagstiftningen inte i tillräckligt hög grad anpassats till EU:s dataskyddsrätt. Att det råder oklarheter om rättsläget försvårar utvecklingsarbetet i staden och kan också påverka invånarnas tillit till de kommunala myndigheterna. De förändringar som kan behövas handlar främst om bättre anpassningar av den svenska lagstiftningen och att använda det handlingsutrymme som medlemsstaterna har enligt GDPR, och inte om en sänkning av skyddsnivån för personuppgifter.

Förord

Alltför sällan tar vi oss an kommunala frågeställningar ur ett mer abstrakt eller filosofiskt perspektiv. Det är synd för det är i det kommunalgrå vi kan hitta de riktiga färgexplosionerna. När vi målar världen i svart eller vitt, tenderar vi att helt missa nyanserna.

Därför är det glädjande att Datalabbet, inom ramen för *Den (ut)forskande staden*, har närmat sig frågan om *kommunala myndigheters delning av invånardata*, ett i dessa dagar ständigt aktuellt ämne, ur inte bara ett tekniskt och juridiskt perspektiv utan även ur ett etiskt perspektiv. Att undersöka helsingborgarnas attityder till hur kommunen använder deras data, handlar om att lära oss mer om den personliga integriteten - och i förlängningen om hur vi ser på vår demokrati. I det närmaste väcks moralfilosofiska frågor som kräver eftertanke och vidare samtal om hur vi tar oss an detta gränsland mellan teknik, juridik och etik.

Inom kommunen är det många som säger att data är *det nya guldet*. Men vilken data är det vi talar om? Och om vi nu laddar data med värde – vem äger *egentligen* de data som kommunen samlar in? Är det den som lämnar från sig data, frivilligt eller ofrivilligt, eller är det den som samlar in invånarnas data? Försöker vi komma undan med en rififikupp med någon annans guld? Detta är intressanta frågeställningar som delvis diskuteras och besvaras i denna rapport, men som vi också behöver diskutera vidare.

En annan ytterst intressant fråga författarna lyfter handlar om den höga *tillit* som invånarna tycks hysa till kommunen och dess arbete med digitalisering. Det finns en stor tilltro till att kommunen agerar både i enlighet med gällande lagstiftning och etiskt korrekt. Den statsvetenskapliga forskningen framhåller tilliten till den offentliga förvaltningen som en av de viktigaste aspekterna för en välfungerande demokrati. Det är detta – tilliten – som ligger i vågskålen när vi raljant ondgör oss över en lagstiftning vi inte tycker har hängt med, eller frågar oss vad som egentligen skulle kunna hända om vi bryter mot någon enstaka föreskrift.

Tilliten och förtroendet är något som vi måste vårda, underhålla och kämpa för – tillsammans – varje dag.

Mathias Johansson Perttu
Servicedirektör, med ansvar för demokratifrågor
Stadsledningsförvaltningen
Helsingborgs stad

DATALABBET:

Att använda invånarnas data i kommunal utveckling

Annika Nilsson

Inledning: Data och välfärdsuppdraget

Digitaliseringen ses som en viktig pusselbit för att lösa den svåra ekvation som den demografiska utvecklingen ställer den offentliga sektorn inför: hur ska allt färre personer i arbetsför ålder kunna upprätthålla välfärd till allt större grupper under 18 år och över 67? Denna utmaning blir än mer påtaglig i en tid där utvecklingen går fort och förväntningarna på den service befolkningen erbjuds ökar. Helsingborgs stad har stora ambitioner när det kommer till såväl digitalisering som innovativt arbete. Det finns en hög tilltro till att digitaliseringen kan bidra till att lösa komplexa samhällsutmaningar inom klimatomställning, stadsbyggnad och välfärd.

Den välfärd kommunen erbjuder berör kommuninvånarna i alla stadier av deras liv, från småbarnsåren till ålderdomen. I alla dessa möten med förskola, skola, stadsplanering, kultur- och idrottsverksamheter, vård, omsorg och sociala insatser, delar invånarna data med staden. För många invånare framstår staden som *en enda sammanhängande* aktör, som har en samlad bild av invånarnas liv och behov.

I verkligheten är dock staden uppdelad i flera olika fristående förvaltningar, som var och en ansvarar för en viss verksamhet. Eftersom varje förvaltning är en egen myndighet som samlar in data för sina behov, begränsar GDPR möjligheten att överlämna data mellan förvaltningarna. En del personuppgifter som invånarna delar med sig av är också känsliga och sekretessbelagda, vilket innebär att det kan finnas begränsningar i hur tjänstepersoner får dela data också inom en och samma förvaltning. Detta gäller till exempel data om enskilda individer inom skola och socialtjänst.

Gränserna mellan förvaltningarna, och begränsningarna i hur data får delas, leder till en fragmenterad bild av invånarnas vardag och behov. För invånarnas del, betyder detta bland annat att de själva måste ansvara för att överföra relevant information mellan olika handläggare och kontaktpersoner. För kommunens del, innebär det att man får en fragmenterad bild av invånaren. Varje förvaltning och varje funktion sitter med sin pusselbit av invånarens livshistoria, utan möjlighet att få en helhetsbild.

I dagsläget innebär alltså kommunens sätt att hantera invånarnas data, att förvaltningarna inte kan samverka effektivt kring invånarnas behov - även om det skulle vara till invånarnas fördel. Det gör det svårt för kommunen att uppfylla förvaltningslagens krav (8§ FL) om såväl samverkansskyldighet gentemot andra myndigheter som serviceskyldighet gentemot invånarna (som slår fast att förvaltningarna i rimlig grad själva ska inhämta uppgifter om den enskilde, så att detta ansvar inte hamnar på invånaren själv).

För att utvärdera och utveckla stadens verksamhet i den takt som behövs för att upprätthålla välfärden, har Helsingborgs stad behov av att använda den data kommunen besitter på nya sätt. Staden ser med andra ord en outnyttjad potential till ny kunskap i den data invånarna delar med sig av. Om data från olika förvaltningar bara kunde kombineras och analyseras på nya relevanta sätt, obero-

ende av förvaltningsgränserna, skulle kommunen få en mer komplett förståelse för invånarnas situation. Därigenom skulle den service staden erbjuder kunna utformas primärt utifrån *invånarnas behov* och inte utifrån *stadens organisering och förvaltningsgränser*.

Om kommunen skulle börja samla in invånarnas data i syfte att använda den samlat och strategiskt, skulle det dock innebära en ny form av intrång i kommuninvånarnas integritet. Även om en sådan samordning skulle leda till bättre kommunal service, är det inte därför säkert att invånarna förstår eller vill ge sitt samtycke till en sådan ökad samordning av data.

De studier som gjorts på nationell nivå, tex Internetstiftelsens årliga undersökning *Svenskarna och internet,* ger viss insyn i svenska medborgares inställning till nationella myndigheters hantering av data, men det saknas kunskap om invånarnas attityder till hur en kommun hanterar deras data på lokal nivå. Kunskap om hur invånarna ställer sig till de etiska dilemman som en samordning av kommunala data medför, blir i hög grad vägledande för stadens arbete. Om invånarna till exempel ger uttryck för en obefogad oro om hur data samlas in och används inom ramen för en ny kommunal tjänst, bör staden arbeta med att förtydliga sin information och utveckla tjänsten så att den är bättre anpassad till, och förankrad hos, invånarna. Om invånarna däremot ger uttryck för en oro som är befogad, bör kommunen av integritetsskäl istället avstå från att utveckla den nya tjänsten.

Det finns även oklarheter kring vad förvaltningarna och kommunen som helhet juridiskt får göra när det kommer till datadelning. Det finns till exempel en konflikt mellan de lagar som ska skydda den personliga integriteten och reglera insamling och delning av data å ena sidan och den samverkansskyldighet som kommunen har enligt Förvaltningslagen å den andra. De juridiska frågorna måste därför redas ut, och kunskapen om vad man får och inte får göra måste spridas till fler tjänstepersoner i kommunen.

Det optimala vore alltså om nya former för att samköra data kunde förena både det offentligas behov av effektivare arbetssätt och individernas behov av anpassad och god service, och samtidigt ske inom ramen för de rättsliga kraven och utifrån väl avvägda etiska ställningstaganden. Om detta är möjligt är dock oklart. Att utforska möjligheterna att arbeta på nya sätt med den data som invånarna lämnar till kommunen ligger alltså i linje med kommunens uppdrag ur flera aspekter. Det var för att kunna genomföra detta utforskande arbete som Datalabbet initierades. Datalabbet hade som ambition att tackla frågan om kommunens service och tjänster från ett nytt håll och startade med utgångspunkten att staden underlåter att göra sitt uppdrag om man inte agerar aktivt och utforskar de här frågorna.

Datalabbets genomförande

Datalabbet pågick 2019-2022 och var en del av det stadsövergripande projektet *Den (ut)forskande staden* som drevs av stadens forsknings- och utvecklingsenhet (FoU Helsingborg) inför stadsmässan H22. *Den (ut)forskande staden* var organiserad i fem hypoteslabb som pågick parallellt, där Datalabbet var ett av dessa labb[1]. Datalabbets projektgrupp bestod av två forskare och två tjänstepersoner från Helsingborg stad som drev det löpande arbetet tillsammans.

De medverkande forskarna var Sara Leckner, docent i medieteknik vid institutionen för dataveten-skap och medieteknik, Malmö universitet och Jonas Ledendal, doktor i handelsrätt vid Ekonomihögskolan, Lunds universitet. Sara Leckner hade fokus på det etiska perspektivet och undersökte invånarnas tillit till kommunen och attityder till datahantering. Jonas Ledendal fokuserade på det juridiska perspektivet och de många lagar som berör kommunal datahantering.

Från Helsingborgs stads sida drevs projektet till en början av Kalle Pettersson, utvecklingschef på Socialförvaltningen. 2021 togs projektet över av Anders Westerlund,verksamhetsutvecklare på Digitaliseringsavdelningen. Annika Nilsson, forsknings- och utvecklingsledare på FoU Helsingborg, medverkade som samordnare under hela projektet.

Datalabbet inkluderade också en arbetsgrupp, bestående av medarbetare som arbetar med datahantering, från stadens förvaltningar och bolaget Helsingborgshem. Denna grupp bidrog till att utveckla problematiken och frågeställningen, tydliggjorde vilken data som finns i stadens förvaltningar och hur den hanteras, samt delade med sig av erfarenheter om juridiska och etiska hinder från tidigare utvecklingsprojekt.

Till projektet knöts även ett Advisory board som träffades tre gånger per år, som gav råd om labbets genomförande och fördjupade analysen tillsammans med labbets forskare. Denna grupp bestod av följande forskare och experter:

- Malin Larsson, Head of Operation, AI Sweden
- Kalle Åström, professor i matematik, Lunds universitet
- Petter Falk, doktorand i statsvetenskap, Centrum för tjänsteforskning, Karlstad universitet
- Stefan Larsson, docent i teknik och social förändring vid LTH, Lunds universitet
- Kalle Pettersson, Senior Policy Designer, Experio Lab

1 Läs mer om Den (ut)forskande staden på fou.helsingborg.se/denutforskandestaden

Datalabbets hypotes och mål

Som ett sätt att knyta ihop praktiken och forskningen i labbet, formulerades en hypotes som skulle utforskas, snarare än en traditionell forskningsfråga. Med en forskningsfråga är risken att ansvaret för att besvara frågan främst hamna på forskarna, medan en hypotes öppnade upp för att utforska området tillsammans. Hypotesen labbet arbetade utifrån var:

> *Genom att samköra och analysera olika invånardata som kommunen samlat in kan komplexa samband upptäckas på en aggregerad nivå. Utifrån dessa insikter kan kommunen utveckla nya offentliga tjänster som bättre svarar mot de komplexa behov som invånarna har.*

Labbet hade en ambitiös målsättningen. Det **primära målet** var att identifiera ett juridiskt gångbart koncept för stordataanalyser baserat på invånardata från två eller fler förvaltningar. Vidare skulle labbet undersöka invånarnas inställning till nya sätt att använda anonymiserade data i designen av förvaltningsövergripande tjänster som syftar till att ge större värdeskapande för invånarna.

Därefter var förhoppningen att kunna presentera 2 till 3 offentliga tjänster som designats utifrån de insikter om invånares komplexa behov samkörningen och attitydundersökningen resulterat i. Om det primära målet inte gick att uppfylla på grund av oöverstigliga juridiska hinder, men invånarnas inställning till att dela data visade sig vara positiv, hade labbet som **sekundärt mål** att försöka påverka lagstiftaren att undanröja de juridiska hindren.

Forskningen i labbet delades upp i två delstudier, en samhällsvetenskapligt och en rättsvetenskapligt, som gemensamt utforskar labbets hypotes. De två delstudierna har kontinuerligt stämts av för att spegla och lära av varandra. Även om de etiska och rättsliga frågorna är beroende av varandra, är det viktigt att skilja etik och juridik åt. Juridiken drar genom legalitetsprincipen upp en yttre ram för vad offentliga myndigheter *får* göra. Det är dock inte självklart att en myndighet alltid *bör* vidta en åtgärd även om detta handlande är tillåtet enligt rättsordningen.

Sara Leckners delstudie utgår från det etiska perspektivet och syftet är att fånga medborgarnas inställning till kommunens nuvarande och önskade dataanvändning. Målet är att ge underlag till *hur* datadriven teknik kan användas på ett etiskt riktigt sätt, utifrån invånarnas perspektiv. De metoder som använts är bland annat enkäter och fokusgrupper.

Jonas Ledendals delstudie utgår från det juridiska perspektivet och syftet är att undersöka de rättsliga förutsättningarna för att dela data mellan kommunala myndigheter samt om de bestämmelser som gäller för kommunala myndigheter utgör särskilda hinder för att dela data och tillhandahålla digitala tjänster till sina invånare. Denna delstudie utgår från det som brukar kallas traditionell rättsvetenskaplig metod eller rättsdogmatisk metod. Detta innebär att frågor om gällande rätts innehåll besvaras genom en rigorös och kritisk analys av vedertagna rättskällor, såsom författningar, förarbeten, rättspraxis och den rättsliga litteraturen.

I första fasen av projektet genomförde projektgruppen tre workshops med arbetsgruppen för att avgränsa och konkretisera det utforskande arbetet. Arbetsgruppen formulerade två så kallade ”livshändelser”, som speglar målsättningen för några av stadens största förvaltningar: skol- och fritidsförvaltningen, socialförvaltningen och arbetsmarknadsförvaltningen. De två livshändelserna var:

- Att elever uppnår kunskapskraven i grundskolan.
- Att invånare avslutar långvarigt ekonomiskt bistånd.

Dessa två händelser har identifierats som två av de enskilt viktigaste faktorer för att bidra positivt till en individs livssituation och möjlighet till egenförsörjning. För de individer som inte klarar kunskapskraven i grundskolan eller långvarigt är beroende av ekonomiskt bistånd finns det oftast många bakomliggande sociala faktorer som bidragit till händelsen och de riskerar också medföra ytterligare komplikationer för individen. På generell nivå finns det mycket kunskap om detta beroendemönster, men förvaltningarna saknar insyn i hur beroendemönstret ser ut mer specifikt för individer och familjer i Helsingborg.

Då livshändelserna har beröringspunkter med flera av stadens verksamhetsområden (bland annat skolan, socialtjänsten, fritid, boende, kultur, sysselsättning) kunde alla deltagare i arbetsgruppen uppge ett dataset som teoretiskt sett skulle vara relevant att dela för att få en större förståelse för en av de två livshändelserna. Labbets forskare kunde i sin tur utgå från livshändelserna och de identifierade dataseten i sina delstudier, för att få en förståelse för hur staden potentiellt skulle kunna använda sin data. Det påverkade bland annat hur Sara Leckner formulerade frågorna i enkäten och vilka speciallagar Jonas Ledendal särskilt fördjupande sig i.

Avgränsning

Även om Datalabbet var ett gemensamt forsknings- och utvecklingsprojekt redogör denna rapport främst för forskningsresultaten från de två delstudierna. Det innebär att arbetet med att utveckla nya offentliga tjänster, där insikter från invånarnas data användes på nya sätt inte kommer redogöras i den här rapporten. Detta utvecklingsarbete har inte kunnat göras inom Datalabbets ramar utifrån de resultat som kom fram i den juridiska delstudien. I stället har Anders Westerlund, som var ansvarig i projektgruppen för stadens utveckling, haft en konsulterande roll gentemot förvaltningarna och löpande återfört lärdomar från Datalabbet in i befintliga projekt för att stötta dem i deras utveckling av nya offentliga tjänster. Den ökade förståelse för GDPR och relaterad lagstiftning innebär att det startats flera utvecklingsprojekt där man analyserar data *inom* respektive förvaltning på nya sätt och även utforskat möjligheterna med anonymisering. Mer information om dessa projekt finns på innovation.helsingborg.se.

Disposition

Utöver denna inledning, är rapporten indelad i tre kapitel. I det första kapitlet presenterar Sara Leckner sin delstudie om invånarnas attityder till delning av data och resultateten från bland annat den enkät och de gruppintervjuer hon genomförde 2021 till 2022. Resultaten presenteras i form av en SWOT-analys som bland annat tydliggör invånarans tillit till Helsingborgs stad, synen på kommunens hanteringen av invånarans data och hur detta påverkas om invånarans data anonymiseras. Hon avslutar med ett antal råd kring vilka etiska förhållningssätt staden bör anamma.

I det andra kapitlet redogör Jonas Ledendal för de rättsliga ramar som gäller när en kommunal myndighet hanterar personuppgifter och delar data med andra myndigheter. Han fördjupar sig också i alternativa metoder, bland annat anonymisering och federerad maskininlärning, som möjliga vägar för att dela data.

I det tredje och avslutande kapitlet lyfter författarna gemensamt ett antal skärningspunkter mellan det etiska och det juridiska perspektivet. Kapitlet avlutas med en diskussion om vilka lärdomar som gjorts i Datalabbet i relation till det praktiska utvecklingsarbetet i organisationen, samt hur staden behöver organisera sig framöver för att ta vara på den kunskap som producerats i Datalabbet.

ETT ETISKT PERSPEKTIV PÅ DATADELNING:

Kommuninvånarnas inställning till delning, hantering och användning av personliga data

Sara Leckner

Inledning

För att kunna skapa nya smarta tjänster som bättre utnyttjar den ökande mängd data som stadens olika förvaltningar samlar in om dig och andra invånare – här kallad "invånardata"– vill vi inom kommunen använda information om dig och andra helsingborgare på sätt som vi inte får lov att göra idag på grund av nuvarande lagstiftning. Det skulle bland annat innebära att med hjälp av AI-analys och automatisering kombinera och koppla ihop stora mängder anonymiserade invånardata som stadens olika förvaltningar har samlat in. På så sätt tror vi att kommunen bättre kan tillgodose er invånares olika behov, även i mer komplexa situationer – både i er nuvarande vardag och genom att kunna förutsäga vissa behov och sätta in åtgärder innan dessa uppstår. Vad tror du om detta? Låter det som något som du tycker att kommunen ska gå vidare med och undersöka närmare?

Så skulle bakgrunden till den här delen av Datalabbet – som utgår från det etiska perspektivet och handlar om kommuninvånarnas inställning till datadelning inom kommunen – kunna formuleras för stadens invånare.

Vad är utmaningen då med den datadelning som beskrivs ovan, sett från ett invånarperspektiv?

Jo, bortser vi från nuvarande lagrum och de begränsningar som finns för att samköra invånardata från olika kommunala förvaltningar, väcker datahantering också frågor kring både etik och personlig integritet. Inte minst har tekniken ifrågasatts som en följd av den tveksamma, och i vissa fall illegala, användningen av personliga data – data som direkt eller indirekt kan identifiera en individ – som uppmärksammats internationellt under det senaste årtiondet. I den offentliga debatten kring sådana data har insamlingen framför allt framställts som ett potentiellt hot mot användarna. Under senare år har därför lagarna för att skydda användarnas integritet skärpts, bland annat med införandet av dataskyddsförordningen (GDPR) 2018. Att lagen ger datainsamlande aktörer utrymme att agera på ett visst sätt, innebär dock inte att insamlingen är önskvärd eller ens lämplig ur ett etiskt perspektiv. För det krävs också att användarna ställer sig bakom idén. Kritiken mot datainsamling har främst rört kommersiell insamling, och främst den insamling som görs av de stora plattformsföretagen. Det finns dock risk att den personliga integriteten kränks även när informationsdelning sker inom och mellan myndighetsinstitutioner, särskilt som den informationen ofta rör känsliga eller närgångna data (SOU 2016).

Även om det kan finnas brister i nuvarande regelverk eller i tillämpningen av dessa, är tolkningsfriheten för vad som kan anses rätt eller gott från ett etiskt perspektiv ännu mer obestämd. Data, och de tekniker som används för att samla in dem, kan varken betecknas som "goda" eller "onda", men inte heller neutrala eller objektiva. Som med all teknik handlar det om vad vi gör med dem och i vilka sammanhang de används. Etiska diskussioner kopplade till ny och framväxande teknikutveckling får dock ofta karaktären av ett dilemma: Är det acceptabelt eller inte att implementera eller tillämpa den här teknologin? Det sätter lätt teknik och samhälle i ett motsatsförhållande och leder inte sällan

in den offentliga debatten mot ett ”antingen eller”: tekniken ska antingen lösa *alla* våra problem *eller* så ska den förkastas. Denna bild är problematisk då teknik och samhälle i grunden är sammanflätade. Teknik utvecklas (oftast) för att fylla en viss roll eller syfte i samhället, och samhället har alltid tagit form genom samspel med teknik, inte sällan på ett sätt eller med ett syfte som inte var tänkt eller planerat från början. Så i stället för att se etik som någon form av ”bedömning” för hur en teknologi kan användas i och av samhället, kan etik i stället ses som en ”vägledning”. Den centrala frågan blir då inte ”ja eller nej?”, utan ”hur?”. Vägledningsetiken fokuserar inte på att förkasta eller acceptera en ny teknik, utan på hur den kan utvecklas, implementeras och användas för att komma så många människor som möjligt till godo (Verbeek & Tijink 2020).

Med utgångspunkt i ovanstående diskussion syftar har den här studien – som en av två delstudier inom ramen för Datalabbet – att fånga invånarna i Helsingborgs stads inställning till kommunens nuvarande och önskade dataanvändning och digitaliseringsarbete, specifikt vad rör AI-baserad samkörning av förvaltningarnas invånardata. Målet har varit att ge Helsingborgs stad underlag för *hur* datadriven teknik kan användas på ett etiskt gott sätt, utifrån invånarnas perspektiv.

Kort om metoden

För att uppnå syftet har fyra undersökningar genomförts inom ramen för delstudien.

- En enkätundersökning bestående av 30 frågor som baserades på ett kvoturval av Helsingborgs stads invånare (18–85 år). Undersökningen genomfördes sommaren 2021 och fick 606 svar. Enkäten undersökte invånarnas kunskap om, och inställning till, insamling och användning av personliga data. Den undersökte också invånarnas inställning till att använda av AI-baserade tjänster, automatiserat beslutsfattande och samkörning av stora datamängder inom kommunen.

- En enkätundersökning bestående av 20 frågor riktad till tjänstepersoner från varje förvaltning i Helsingborgs stad som har en funktion kopplad till digitalisering. Undersökningen genomfördes våren 2021 och gav totalt 12 svar (1-2 från varje förvaltning). Enkäten undersökte kommunens inställning till brukarnas kunskap om, och inställning till, insamling och användning av personliga data, och utgjorde ett komplement till de övriga undersökningarna.

- En undersökning av invånarnas reaktioner på sex påståenden om delning av personliga data med kommunen. Påståendena publicerade på Helsingborgs stads sociala mediekanaler (Facebook och Instagram) under två veckor, senvåren 2021. Undersökningen genererade cirka 30 gillamarkeringar och 10 kommentarer.

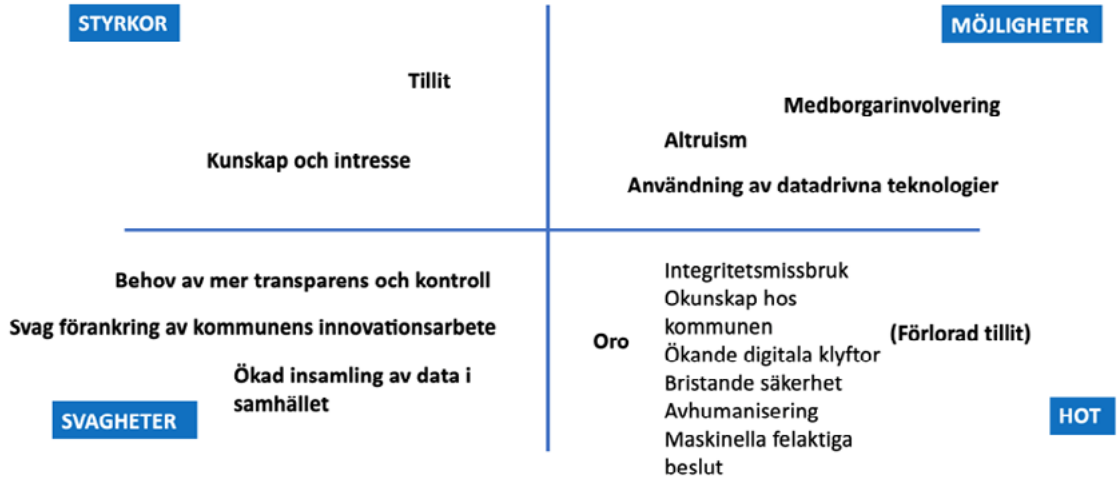
- Fyra fokusgruppintervjuer (à 2h) med totalt 25 personer (25–80 år), baserade på ett bekvämlighetsurval av Helsingborgs stads invånare (18+ år). Undersökningen genomfördes under våren 2022. Syftet var att undersöka invånarnas tillit till kommunens hantering av invånardata och deras inställning till samkörning och anonymisering av sådana data.

Resultaten från undersökningarna ligger till grund för innehållet i detta kapitel och fokuserar på det som ansetts speciellt värdefullt för kommunens fortsatta arbete med invånardata. För mer detaljerade redovisningar av resultaten hänvisas till följande texter:

- Leckner, S. (2022). Delning av invånardata från ett användarperspektiv. I A-K. Bergman & M. Adenskog (red.), *Den (ut)forskande staden: En FoU-innovation i offentlig sektor.* Helsingborg: FoU Helsingborg, 193-217.
- Leckner, S. (Kommande). Legitimate or not: Assessing trust as a criterion for sharing personal data.
- Leckner, S. (Kommande). Preserving Privacy: The significance of anonymization in data sharing with private and public sectors.

Resultat

För att tydliggöra invånarnas åsikter och inställningar till kommunens nuvarande och önskade dataanvändning och digitaliseringsarbete, visualiseras resultaten från studiens undersökningar genom en SWOT-analys. Det möjliggör en bedömning av de styrkor, svagheter, möjligheter och hot som kommunen står inför i sitt fortsatta digitaliseringsarbete. SWOT-analysens resultat illustreras i figur 1, där varje del redogörs för i kapitlet.



Figur 1. De styrkor, svagheter, möjligheter och hot som utkristalliserats från resultaten av delstudiens undersökningar och presenteras i detta kapitel.

Styrkor

De styrkor som identifierades i resultaten var invånarnas **tillit** till kommunen som helhet, inklusive dess hantering av invånardata, samt invånarnas **kunskap om och intresse** för dessa frågor.

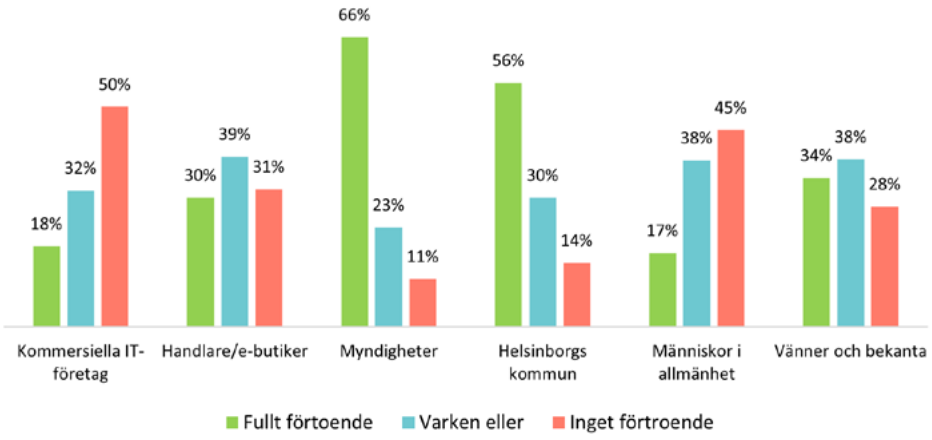
Invånarnas tillit till kommunens digitaliseringsarbete

I studiens undersökningar framkom att kommuninvånarna hyser en hög grad av tillit till kommunen och dess arbete med digitalisering. Detta är mycket viktigt då tillit – ofta använt synonymt med förtroende – är en avgörande komponent för ett välfungerande samhälle (Trägårdh m fl 2013). Ökad ojämlikhet i ett samhälle kan ofta kopplas till en lägre tillit. Den höga tilliten till Helsingborgs kommun kan delvis relateras till det svenska samhället i stort. Sverige är, tillsammans med övriga nordiska länder, ett av få så kallade högtillitsländer: länder där medborgarna hyser hög tillit till staten, dess institutioner och sina medmänniskor. Även om det finns tecken på en långsiktig minskning av tilliten till statliga institutioner (Holmberg & Weibull 2017) och det finns en betydande variation i tillitsgraden mellan Sveriges kommuner (Trägårdh m fl 2013), är samhällstilliten fortfarande hög i Sverige jämfört med i andra europeiska länder (Regeringen 2018[2]).

Vid en uppskattning av vilka aktörer helsingborgarna hade förtroende för vad gäller hantering av deras data, kom myndigheter och kommunen i topp (se figur 2). I botten hamnade plattforms- och It-företag, som exempelvis sociala medier och söktjänster, vilket överensstämmer med nationell statistik (Internetstiftelsen 2019). Bristen på tillit till sådana aktörer beror på att invånarna upplever att de har oklarare processer och regler för insamling och hantering av data. Stat och kommun anses däremot vara både mer etiska och juridiskt korrekta i sin hantering av data. Lagrummet kring insamling och användning av insamlade data är också striktare för stat och kommuner än för kommersiella företag.

Resultaten visar således att den hårdare regleringen och den etiska efterlevnaden är en viktig grund för kommuninvånarnas nuvarande tillit till kommunen. *Vad* dessa lagar och regler innebär mer konkret är det dock få invånare som vet, eller är intresserade av att veta. Exempelvis trodde alla fokusgruppdeltagarna (inklusive författaren till detta kapitel) att kommunen redan får samköra invånardata från olika förvaltningar och också gör det.

2 Uppgiften gäller Sveriges placering i Världsbankens index *Government Effectiveness* samt i organisationen Transparency Internationals *Corruption Perceptions* Index.



Figur 2. Helsingborgarnas förtroende för hur olika aktörer hanterar deras personliga data.

Däremot visar resultaten att den mellanmänskliga tilliten – det vill säga tilliten till andra människor– liksom den partikulära (intima) tilliten – den till nära och kära – inte är lika hög. Helsingborgarna litar mer på myndigheternas och kommunens datahantering än vad de gör på sina närståendes och andra medmänniskors. Därmed tycks den vertikala tilliten – till staten och dess institutioner – vara hög även när det gäller datahantering, medan den horisontella tilliten – den mellan människor – inte är lika hög. Det ska påpekas att den så kallade lokalsamhällestilliten även i andra studier har visat sig vara lägre i Helsingborg jämfört med i många andra kommuner i Sverige (Tillitsbarometern 2021). Detta innebär att helsingborgarnas tillit till att kommunen i olika stadsdelar i lokalsamhället förmår upprätthålla trygghet, rättigheter och social service, är lägre än riksgenomsnittet. Det innebär också att helsingborgarna har mindre tillit till människor i det egna närområdet. Detta skulle också kunna vara en förklaring till den något lägre tilliten till kommunens datahantering, jämfört med den tillit helsingborgarna tillskriver andra myndigheter.

Vad behöver Helsingborgs stad då göra för att invånarna ska känna sig trygga med att dela sina data?

- I topp ligger enkel och tillförlitlig information som förklarar syftet med dataanvändningen. Det är också viktigt att kommunen inte överlåter personliga data till andra aktörer utan tillåtelse. Det senare ska ses som en sorts ”samtycke” som bör inhämtas på olika sätt för hur kommunen avser använda de data de samlar in (även om statliga institutioner inte använder samtycke på samma sätt som kommersiella aktörer). Som jämförelse vid delning med kommersiella aktörer anses deras försäkran om att data inte ska överlåtas som långt viktigare än att syftet med inhämtningen förklaras (Larsson m fl 2020). Samtidigt tycks helsingborgarnas önskade informations-

insatser främst handla om åtgärder som kräver mindre engagemang hos invånaren, då exempelvis kontakt eller kundtjänst (fysisk som digital) som kan svara på frågor inte var lika efterfrågad.

- Viktigt, men mindre förväntat, var att en relativt hög andel invånare ansåg att hög datasäkerhet hos kommunen var viktig, en aspekt som inte varit lika framträdande i nationella studier. I efterhand är det mindre förvånande, då hög tillit hänger ihop med att man också litar på att aktören som samlar in data kan förvalta dem så att inte obehöriga kommer åt dem. Eftersom enskilda personer har små möjligheter att påverka hur deras uppgifter hanteras är det nödvändigt att data hanteras säkert, inte minst då kommunala data kan innehålla känsliga och sekretessbelagda uppgifter.

- En aspekt där svaren gav en annan bild än förväntat, var att invånarna lade liten vikt vid anonymisering av data. Många helsingborgare ansåg att anonymisering var mindre viktigt än andra aspekter de fick ta ställning till om vad som påverkade tilliten till datadelning (se figur 7). Detta diskuteras mer under rubriken anonymisering.

Tillit innebär att individen gör sig sårbar genom att ge någon annan kontroll (t ex Warren 1999), vilket ställer krav på den man överlåter kontrollen till. Att invånarna litar på ett system (jämför exempelvis med när man kör bil eller genomför monetära transaktioner), och inte i varje situation behöver överväga hur man ska gå till väga, förenklar vardagen. Samtidigt är det inget självändamål att invånarna litar blint på kommunen. Missriktad tillit är lika problematisk som brist på tillit. I en välfungerande demokrati finns det skäl, och är hälsosamt, att ifrågasätta. Att kunna ifrågasätta är viktigt för aktivt deltagande i den demokratiska processen och för god medborgardialog (se också avsnitten om medborgarinvolvering nedan). Vidare förutsätts att tillit bör gå åt båda hållen, det vill säga, att tjänstepersoner hos kommunen även litar på medborgarna.

Det förtroende som helsingborgarna hyser för kommunens och dess datahantering är naturligtvis viktig att förvalta. Ett förlorat förtroende är svårt att återfå (Trägårdh m fl 2013) och människors tillit till offentlig förvaltning är en av det viktigaste aspekterna i en välfungerande demokrati (Rothstein 2022).

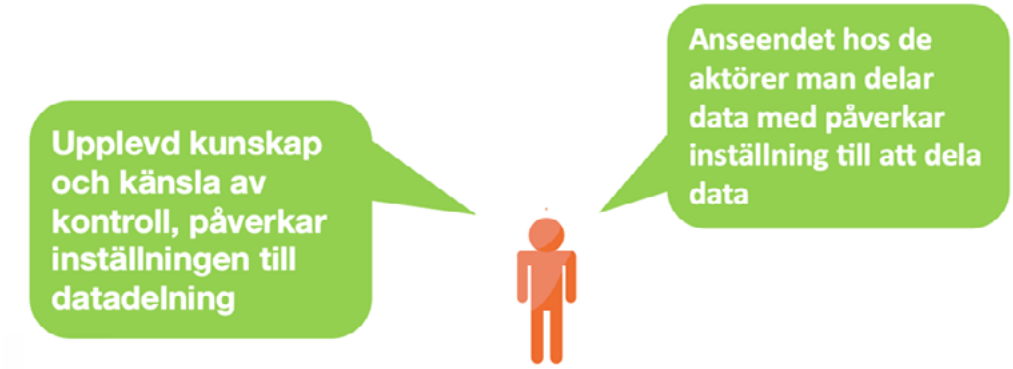
Kunskap och intresse

En ytterligare styrka i kommunens arbete med digitalisering är kommuninvånarnas upplevda kunskap och intresse för datainsamling och datahantering, vilket indikerar en växande teknikmognad. Många helsingborgare anser sig ha goda kunskaper om vad personliga data är och vad datadelning innebär. De är också intresserade av hur deras data samlas in och används (se tabell1).

Tabell 1. Helsingborgarnas kunskap och intresse av datainsamling generellt.

	Instämmer	Varken eller	Instämmer ej
Har god kunskap om vad personliga data innebär	57%	29%	14%
Har god kunskap om hur och när mina data samlas in	44%	33%	23%
Är intresserad av hur data om mig samlas in och för vilka syften	62%	25%	13%
Har god kunskap om vad GDPR innebär	48%	30%	22%
Begränsar den information jag lämnar ut om mig själv [till olika aktörer på internet]	52%	34%	14%

Högre kunskap om vad datahantering innebär och hur man ska göra för att skydda informationen man delar om sig själv, har visat sig korrelera med en mer positiv inställning till datadelning (Leckner 2018a). Har man mindre kunskap om ett fenomen, är det svårare att veta vad det innebär eller vilka konsekvenser det kan få. Detta kan medföra en skepsis och avoghet mot det man saknar kunskaper om. Negativa reaktioner har visat sig innebära större anseenderisker då människor reagerar mycket starkare på negativa upplevelser än på motsvarande positiva (Kahneman & Tversky 1984). Helsingborgarnas upplevda kunskapsnivå är därmed en styrka för kommunens fortsatta digitaliseringsarbete.



Figur 3. Faktorer som påverkar en positiv attityd till datahantering.

Denna kunskapsnivå var dock inte helt förväntat med tanke på Helsingborgs stads befolkningsprofil. Helsingborg har en befolkning med något lägre medelinkomst och utbildningsnivå än riket generellt (Helsingborgs stad 2020) och resursstarka grupper tenderar att ta till sig innovationer snabbare än resurssvaga grupper. Bland annat har lågutbildade och låginkomsttagare, tillsammans med äldre, lyfts fram som potentiella riskgrupper för digitalt utanförskap (Internetstiftelsen 2019).

Anledningen till den högre kunskapsnivån kan bero på det mångåriga digitaliseringsarbete som kommunen genomfört. Det arbetet har bland annat inneburit kunskapshöjande insatser, som kan ha börjat få genomslag hos olika invånargrupper. Samtidigt ska man vara medveten om att metoderna som används i denna studie baseras på självupplevda kunskaper, vilka kan skilja sig mot faktiska kunskaper. En felaktig bild av den egna kunskapsnivån kan exempelvis uppstå hos personer som har mindre kunskap i en fråga, och som därför inte har förmågan att se att de också överskattar sina kunskaper och/eller förmågor, den så kallade Dunning–Kruger-effekten (Kruger & Dunning 1999). Indikation på sådan överskattning i resultaten kan vara att trots att närmare hälften upplevade sig ha goda kunskaper om vad data är och när de samlas in, var det (bara) något fler än hälften som trodde att kommunen samlar in data om dem när de använder kommunens (digitala) service och tjänster. Nationellt är det betydligt fler (91 procent) som tror att olika aktörer samlar in data om dem på nätet (Insight Intelligence 2020). Att data samlas in är ett faktum i det digiatala samhället. Det är dock inte lätt för någon att veta *när* ens data samlas in och det gäller inte bara Helsingborgs stads datainsamling.

Det ska också påpekas att trots att majoriteten av deltagarna i de olika undersökningarna uppgav och gav intryck av att ha generellt goda kunskaper om vad datainsamling och dataskydd innebär, visade fokusgruppernas fördjupade diskussioner att när man skrapar på ytan eller presenterar nya tekniker och nya sätt att använda data på – som AI-baserad samkörning – är det svårt för invånarna att förstå innebörden och konsekvenserna av dem, både från ett integritetsperspektiv och ett nyttoperspektiv. Den upplevda kunskapen rör sig därmed inte om någon djupare kunskap (hos de flesta). Sådan kunskap är dock inte något man kan förvänta sig av gemene man.

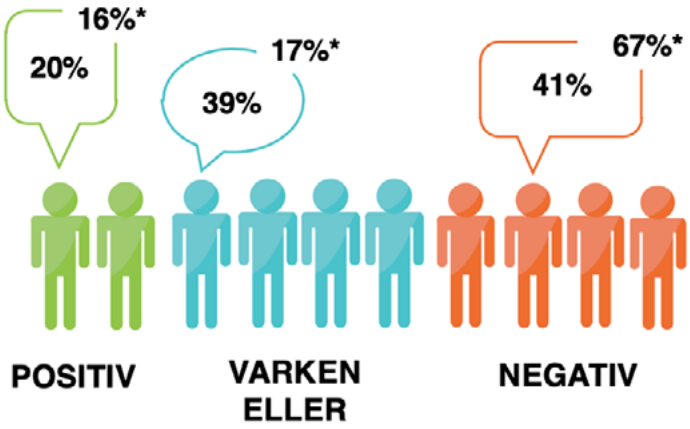
Med förbehållet att resultaten baseras på självuppskattade kunskaper, visar helsingborgarna indikationer på god teknikmognad vilket är en styrka för det fortsatta digitaliseringsarbetet. Vill man veta hur invånarnas faktiska kunskaper ser ut, behöver man studera detta med andra metoder. Oavsett kunskapsnivå, finns det anledning för kommunen att fortsätta arbeta med att tydliggöra när och hur datainsamling sker, och framför allt hur hanteringen av data kommer invånarna till godo, så invånarna kan göra informerade val.

Svagheter

I studien identifierades också ett antal brister eller svagheter, som riskerar att göra kommunens fortsatta digitaliseringsarbete svårare. De identifierade bristerna var invånarnas kritiska inställning till den **ökande datainsamlingen** i samhället och deras avvaktande inställning till **Helsingborgs stads innovationsarbete**, samt behovet av ökad **transparens** kring hur personliga data samlas in och används och mer **kontroll** över detta.

Negativ inställning till ökad datainsamling i samhället

En svaghet för kommunens fortsatta digitaliseringsarbete är att de flesta helsingborgare, liksom majoriteten av den svenska befolkningen, är negativa till den ökande användningen av personliga data i samhället i allmänhet, även om det är fler helsingborgare som inte tar ställning (det vill säga är vare sig positiva eller negativa), jämfört med den svenska befolkningen i stort (Insight Intelligence 2021), se figur 4.



Figur 4. Inställning till ökad insamling och användning av personliga data. *Nationella resultat för jämförelse (Insight Intelligence 2021).

Dessa resultat rör datainsamling generellt och är inte kopplad till någon specifik kontext eller aktör. På en direkt fråga om *kommunens* insamling och hantering av data innebär främst risk eller nytta, var det något fler invånare som såg det som nytta än som risk (31 respektive 21 procent). De flesta (48 procent) svarade dock varken eller. Detta trots att kommunens (liksom andra aktörers) insamling och användning av personliga data, åtminstone officiellt, främst syftar till att öka effektiviteten, nyttan och tillfredsställelsen för användaren. Här finns alltså mer att göra för att invånarna ska uppleva datainsamling som värdefull och trygg.

Avvaktande inställning till kommunens digitaliseringsarbete

En annan identifierad svaghet är invånarnas avvaktande attityd till kommunens arbete med innovation och digitalisering rent allmänt.

Helsingborgs stad har under många år drivit ett fokuserat innovations- och digitaliseringsarbete, som bland annat omfattat projekt som Datalabbet. Kommunen har också i olika sammanhang lyft fram staden som innovativ och i framkant när det gäller digitalisering. För att undersöka hur invånarna ställer sig till detta arbete, fick de ta ställning till ett antal påståenden om innovations- och digitaliseringsarbetet som kommunens gjort hämtade från uttalanden i bland annat media (se figur 5).

Figur 5. Påståenden Helsingborgs stad gjort kring sitt innovation- och digitaliseringsarbete som invånarna fick ta ställning till.

Inget av påståendena genererade ett högt instämmande, utan det var jämnt fördelat mellan de som instämde och de som inte gjorde det. Invånarna tycks därmed inte lika övertygade som delar av stadens organisation om att de bor i en kommun som ligger i framkant vad gäller innovation och digitalisering. Som nämns ovan är helsingborgarna också oeniga i sin syn på riskerna respektive nyttan med kommunens digitalisering och ökade användning av datahantering. Denna splittring återspeglas i de ganska blandade uttalanden kring detta som gjordes i studiens olika undersökningar, exemplifierat i figur 6.

Figur 6. Exempel på invånarnas skiftande åsikter om risker och nyttor med kommunens arbete med bland annat datahantering.

Även om helsingborgare anser sig ha en god teknikmognad och vara mer välvilligt inställda till dataanvändning än svenskarna generellt, tyder detta på att det är färre som är medvetna om, eller intresserade av, kommunens innovativa utvecklingsarbete och vad det innebär. Värdegemenskapen – det vill säga i vilken mån kommunen och dess invånare delar samma målsättning – skulle därmed behöva stärkas kring dessa frågor. Intressant nog visar denna studie att även tjänstepersoner som arbetar med frågor relaterade till digital utveckling i de olika förvaltningarna var förvånansvärt avvaktande och försiktiga i sin återkoppling om vilka behov deras brukare har vad gäller datahantering, vilket kan tolkas som en osäkerhet kring dessa behov och en brist på förankring och diskussion om detta i organisationen.

Kommunens fleråriga arbete med digitalisering och med att förankra utvecklingsarbetet, är en pågående process, men behöver stärkas både inom och utanför organisationen. I nuläget både förväntar sig och förväntar sig inte invånarna att kommunen ska gå i bräschen för innovation.

Brist på transparens och behov av ökad kontroll

En ytterligare svaghet som identifierades var upplevelsen av bristande transparens och kontroll kring kommunens datainsamling och hantering. Synen på personlig integritet handlar i många fall om rätten att kunna kontrollera utflödet av personlig information (Westin 1967). Avsaknad av kontroll anses vara en av de viktigare orsakerna till oro och en kritisk attityd till datadelning (Malhotra m fl 2004). Trots goda kunskaper om datadelning, upplevde bara 27 procent av helsingborgarna att de har kontroll över hur deras data samlas in och används (av även andra aktörer än enbart kommunen). Något fler ansåg sig veta hur de kan undvika att dela data om de vill, och majoriteten begränsar de data de lämnar ut om sig själva (se tabell 2), vilket kan ses som en typ av kontroll. Många invånare kontrollerar därmed sina data på olika sätt, men upplever inte att det som tillräckligt.

Tabell 2. Helsingborgarnas upplevelse av kontroll över de data de delar med olika aktörer online.

	Instämmer	Varken eller	Instämmer ej
Har kontroll över hur mina data samlas in och används	**27%**	**31%**	**42%**
Har möjlighet att avstå från att dela data om jag vill	**37%**	**31%**	**32%**
Begränsar den information jag lämnar ut om mig själv	**52%**	**34%**	**14%**
Gör aktiva val för att kunna surfa anonymt	**36%**	**30%**	**34%**
Användarvillkor och samtycken ökar min kontroll över mina data	**34%**	**36%**	**30%**
Läser noga igenom användarvillkor och samtycken	**32%**	**28%**	**40%**

Trots att helsingborgarna, liksom svenskarna generellt (Leckner 2018b), inte upplever sig ha kontroll över sina data, är det inte alla som aktivt vidtar åtgärder för att begränsa eller ta reda på vilka data de lämnar ut. Det är färre än hälften av invånarna som instämmer i att de använder inställningar för att surfa anonymt, som läser användaravtal och aktivt ger eller avslår samtycke (tabell 2). Detta kan bero på flera saker, exempelvis att man inte vet hur man ska göra eller inte aktivt agerar på sin kunskap. Det senare är viktigt, då upplevelsen av kontroll kanske inte främst handlar om att ha kontroll i faktisk mening, något som ställer höga krav på tekniska mekanismer. Snarare handlar det om vilket *handlingsutrymme* man upplever sig ha över att kunna reglera vad som är privat respektive publikt, *om man skulle vilja* (se Bylund 2013). Detta förutsätter att man kan avgöra om man har ett behov av det och vet hur man i så fall ska gå till väga. Handlingsutrymme kan skapas på många olika sätt, som tydligare information, bättre gränssnitt, fler möjligheter att ändra inställningar. Att öka invånarnas handlingsutrymme är viktigt för viljan att dela data. Se figur 7 för vilka aspekter som gör att invånarna känner sig trygga(re) att dela sina data med kommunen.

På ett enkelt och tillgängligt sätt förklarar vad mina data används till	Garanterar att inte överlåta min information till andra utan mitt samtycke	Förklarar hur jag kan korrigera eller ta bort mina data som samlats in	Ha en tydlig säkerhetsprofil	Förklarar vilken nyttan är för mig med att dela min information	Har tydliga etiska riktlinjer för hur personlig information hanteras	Avidentifierar min personliga information	Erbjuda lättillgänglig kontakt/kundtjänst som kan svara på frågor om datahantering
53%	**39%**	**36%**	**36%**	**29%**	**24%**	**20%**	**13%**

Figur 7. Aspekter som gör att helsingborgarnas känner sig trygga(re) att dela sina data med kommunen.

Men att på förhand kunna bestämma om och hur personliga data ska få användas eller inte, om de ska vara privata eller publika, är inte alltid relevant eller ens möjligt. Viljan till att dela data är i många fall kontextuell (Nissenbaum 2010): ändras förutsättningarna kan också inställningen till att dela data ändras. Exempelvis kan det kännas godtagbart att dela data med en aktör som kommunen (eller en förvaltning inom kommunen), men inte om kommunen i sin tur delar (eller säljer) data vidare till någon annan (jfr Larsson m fl 2020; Leckner 2018a; 2018b). Detta bör kommunen förhålla sig när de utvecklar förvaltningsgemensam samkörning av invånardata. Kan det finnas alternativ som gör det möjligt för invånarna att avstå från att dela sina data eller att senare kunna ta bort dem innan de samkörs om de så önskar (jfr GDPR)? Detta är naturligtvis inte så lätt om data redan används i anonymiserad och aggregerad form i en tidigare analys eller redan spridits för samkörning hos olika förvaltningar.

Sammanfattningsvis handlar de identifierade svagheterna – invånarnas skepsis mot ökad datainsamling i samhället, till kommunens innovationsarbete, och önskade behov av mer handlingsutrymme i sin datadelning – om att kommunen behöver öka förståelsen för digitaliseringsarbetets kvaliteter. Kommunens digitaliseringsarbete bör fortsatt handla om att stödja invånarna kännedom och kunnande om de möjligheter och begränsningar som digitaliseringen innebär för relationen mellan den offentliga förvaltningen och invånarna, så att de, som individer och kollektiv, kan vara med och påverka kommunens digitalisering på ett medvetet och tryggt sätt. Att invånarna är positiva ska inte innebära att de är odelat okritiska. Men uppfattas digitaliseringen innebära kvaliteter som är högt värderade av invånarna, kan det sannolikt öka förtroendet för kommunens förvaltning, och det motsatta om det inte gör det (se Denk m fl 2019).

Möjligheter

I resultaten identifierades också ett antal möjligheter för kommunens fortsatta digitaliseringsarbete. En av dessa är den möjliga **användningen av framväxande teknologier** (inklusive hur den ska hanteras, som **anonymisering**). Även om invånarna i nuläget inte är odelat positiva till all ny teknik, och inte heller alltid förstår vad den innebär, tycks de hysa tilltro till att ny teknik kan gynna kommunen, speciellt om användningen förklaras. Tilltro till ny teknik är en faktor som kan vara avgörande för att uppnå ökad användning (Regeringen 2021). Två andra viktiga möjligheter är **medborgarinvolvering** som kan förstärka förståelsen för hur ny teknik ska eller kan användas, liksom att digitaliseringen anses komma samhället som helhet till godo (**altruism**).

Nyfiken inställning till kommunens användning av framväxande teknologier

Artificiell intelligens (AI) ligger till grund för mycket av den datadrivna utvecklingen. AI kan, beroende på teknikval och design, skapa möjligheter till mer eller mindre autonoma processer. Inom kommunen kan AI-teknik användas vid planering och uppföljning, till exempel genom förvaltningsgemensam samkörning av stora mängder invånardata (se avsnitt nedan som specifikt tar upp detta), som bland annat kan användas för att träna program till att göra prediktioner eller synliggöra mönster i existerande data. AI-teknik kan också användas för olika typer av automatisering som automatiserat beslutsfattande. Vidare kan den användas för interaktion med, och stöd i, offentliga tjänster,

till exempel i form av chatbots som ger information och stöd, robotar inom hälsa och sjukvård eller appar som kan ge råd om lokaltrafik eller kulturhändelser baserat på vem man är och hur man lever. Att använda framväxande teknologier som automatiserat beslutsfattande och andra AI-tjänster, skulle öppna upp nya möjligheter i kommunens digitaliseringsarbete. Därför tillfrågades invånarna också om sin syn på automatiserat beslutsfattande och AI-baserade tjänster i allmänhet, förutom inställningen till kommunens önskade samkörning genom AI-baserad analys. Nedan redovisas hur invånarna i Helsingborgs stad ställer sig till dessa tekniker och de möjligheter de skapar.

Automatiserat beslutsfattande

Närmare hälften (47 procent) av de invånare som deltog i invånarenkäten, menade att automatiserat beslutsfattande i kommunens verksamheter skulle leda till mer opartiska beslut. Däremot trodde majoriteten av dem inte att det skulle innebära att besluten blev mer tillförlitliga. Det finns med andra ord en skepsis till att automatiserat beslutsfattande skulle säkerställa korrekta och rättssäkra beslut. Vidare ansåg de flesta att en automatisering skulle ge mindre insyn i hur beslut fattas hos kommunen och att det fanns en risk att besluten skulle ta mindre hänsyn till människors olika situationer.

Dessa resultat ligger i linje med nationella data (Denk m fl 2020) även om helsingborgarna är något mer positiva till kommunens automatisering än vad svenskarna är generellt. Riksrevisionens (2020) granskning av automatiserat beslutsfattande hos myndigheter visar att i de flesta fall leder automatiserat beslutsfattande till ökad effektivitet och rättssäkerhet. Granskningen visar dock samtidigt att de fel som uppstår kan få stora konsekvenser för enskilda individer och minska tilliten till myndigheter. Vidare visar rapporten att det görs en alltför begränsad uppföljning av att beslut som fattats automatiserat blivit korrekta. Detta speglas också i mycket av den oro som helsingborgarna uttrycker (se avsnittet om Hot nedan).

I dagsläget använder inte Helsingborgs stad automatiserade beslut på grund av det oklara rättsläget. Denna möjliga användning av ny teknik är den som invånarna är mest skeptiskt till av de tekniker som undersöktes i denna studie, och skulle behöva förankras mer hos invånarna.

AI-baserade tjänster

Bland helsingborgarna ansågs användningen av AI-baserade kommunala tjänster framför allt som värdefulla när de används för samhälls- och vardagstjänster som gör livet enklare och mer effektivt för invånarna. De såg mindre nytta med att använda AI-teknik för att skapa service och rekommendationer anpassade till den enskilda individen. Detta återspeglades också i invånarnas bedömning av i vilka verksamheter användningen av AI-tjänster skulle vara till mer eller mindre nytta. Användningen av AI-tjänster ansågs ge störst nytta inom kollektivtrafik, trafikplanering och planering av stadsmiljön, men mindre nytta i sjukvård, barnomsorg, äldreomsorg och sociala insatser.

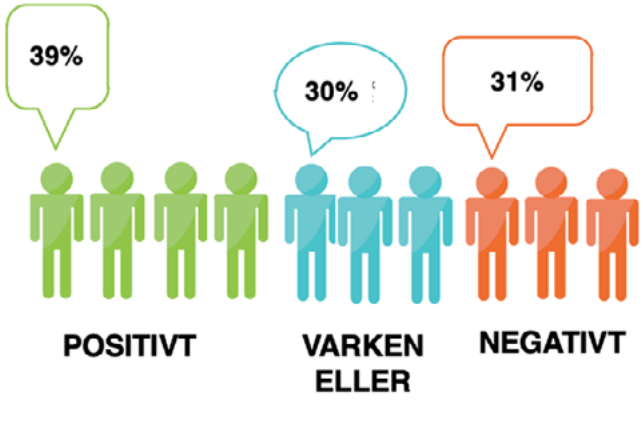
Det ska poängteras att AI kan användas på många olika sätt inom olika verksamheterna. Resultaten ger bara en övergripande indikation på invånarnas inställning och bör följas upp med mer speci-

fikt riktade undersökningar. Vidare är det svårt att fråga människor om inställningen till ny teknik, eftersom kunskapen om vad tekniken innebär kan variera. Bland deltagarna i invånarenkäten var det relativt jämnt fördelat mellan dem som sa sig ha hög respektive låg kunskap om vad AI-teknologi innebär (36 respektive 29 procent).

AI-baserade tjänster innebär en stor möjlighet för kommunens digitalisering, men kräver mer tillvänjning och förankring hos invånarna, då 15 procent av de som svarade på invånarenkäten var negativa till all form av AI-användning inom kommunen och lika många var tveksamma eller svarade att de inte hade någon åsikt.

Samkörning

Att det är svårt att fråga om inställning till ny teknik avspeglade sig också i svaren kring inställningen till samkörning av anonymiserade invånardata. Som nämns ovan, visade resultatet från fokusgrupp-undersökningen att alla deltagare förutsatte att kommunen idag redan samkör data mellan förvaltningarna. I fokusgrupperna diskuterades också skillnaden mellan samkörning av stora datamängder och andra former av analys där data jämförs. Till exempel funderade deltagarna över på vilket sätt automatiserad samkörning av stora datamängder skiljer sig från den form av ”samkörning” som när tjänstepersoner från olika förvaltningar diskuterar personliga uppgifter om en invånare på ett möte, eller när olika data samkörs (exempelvis korreleras) för att sammanställa statistik. Även invånarenkätens resultat (se figur 8) tyder på att respondenterna hade svårt att förstå vad samkörning skulle innebära, även om det förklarades kortfattat. Inställningen till samkörning verkar därför inte bero på om man tyckte idéen som sådan var bra eller inte, utan snarare på om man redan hade hög tillit till kommunen som datahanterare.



Figur 8. Helsingborgarnas inställning till samkörning av stora mängder av förvaltningarnas invånardata.

Sammanfattningsvis kan följande slutsatser dras om invånarnas inställning till samkörning:

- Invånarna tror redan att kommunen samkör förvaltningsdata, och upplever inte något integritetsproblem med det.

- Invånarna förstår inte riktigt vad samkörning innebär. Det visar på svårigheten med att fråga om framväxande teknologier och ännu icke existerande nya tjänster som baseras på sådana tekniker (se avsnittet om medborgarinvolvering nedan). Det är svårt för människor att ta ställning till hypotetiska aspekter.

- När fokusgruppsdeltagarna fick större förståelse för vad samkörning kunde innebära, blev de mer positiva. Därmed är det viktigt att sprida information om när, varför och hur kommunen använder data för nya datadrivna tjänster även i presumtivt syfte.

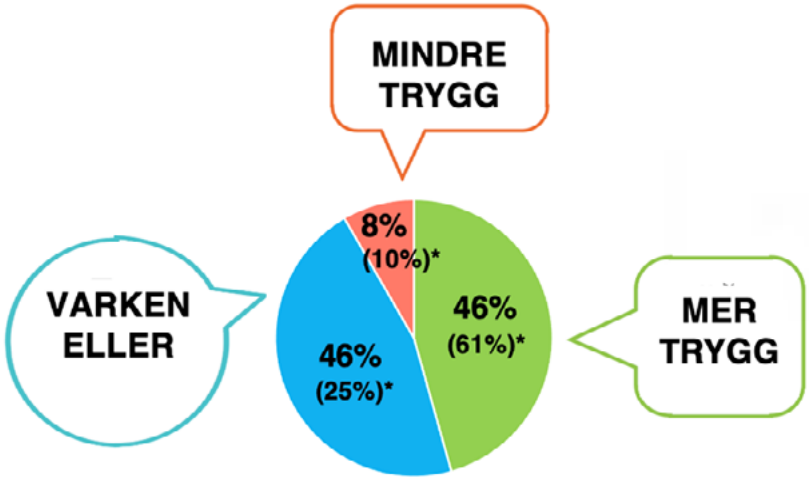
- Spontant ansåg de som deltog i enkäter och fokusgrupper att den främsta nyttan med att samköra data är att det ökar kommunens möjligheter att upptäcka bidragsfusk och andra missbruk av systemet. Noterbart är att vid Riksrevisionens (2020) granskning av automatiserad datahantering hos myndigheter, var en uppmärksammad brist just hanteringen av ärenden med hög risk för fusk och fel.

Möjligheter med anonymisering och individanpassning

Frågan om anonymisering (eller avidentifiering) är viktig. Kommunens idé om samkörning av förvaltningsdata bygger på att använda anonymiserade invånardata. En av anledningarna är att det är juridiskt enklare då sådana data inte omges av samma strikta lagkrav som när data kan kopplas till enskilda individer. Även om individanpassade tjänster har stort värde för användare, kan användningen av anonymiserade data innebära ett snabbare sätt att kunna erbjuda tjänster som är ”bra nog” för många.

En hypotes som denna studie utgick ifrån, var att om kommunen använde anonymiserade data skulle det kunna minska, eller till och med eliminera, den oro som nationella studier visat finns kring att dela data (Leckner 2018a; 2018b). Även om det finns många, framför allt tekniska och administrativa utmaningar med att anonymisera data, har nationella studier visat att användarnas känsla av trygghet ökar om de vet att informationen inte går att spåra tillbaka till dem (Insight Intelligence 2020), se figur 9.

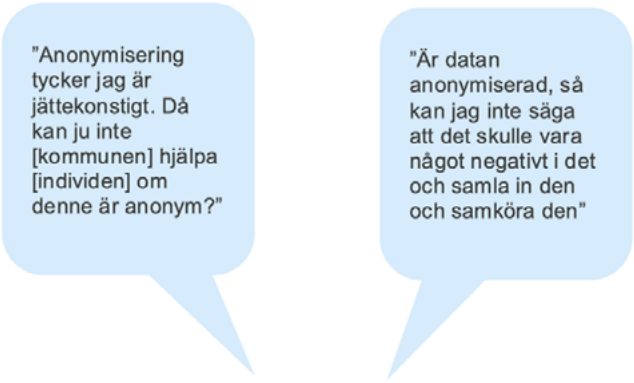
Resultaten från denna studie visade att, tillsammans med andra faktorer som ansågs kunna påverka tryggheten att dela data, ansågs anonymisering inte särskilt viktig (se figur 7). När invånarna fick en specifik fråga om hur anonymisering påverkade tryggheten att dela data, var det dock fler som ansåg att det ökade tryggheten, men lika många som tyckte att det inte spelade någon roll, se figur 9.



Figur 9. Upplevd trygghet vid anonymisering av data. *Nationella resultat för jämförelse inom parentes (Insight Intelligence 2020).

En anledning till resultaten kan vara att känslan av trygghet är beroendet på i vilket sammanhang och med vilken aktör man delar data. I de nationella studierna har frågan inte varit kopplad till en specifik kontext (som i denna studie som rör kommunen). Eftersom debatten kring olika integritetsproblem nästan enbart rört kommersiella aktörers insamling av data, är det sannolikt också den typen av delning som respondenterna tänker på när de har svarat på frågan i studierna med nationellt urval.

I fokusgrupp-undersökningen i denna studie uttrycktes till och med en förväntan på att data *inte* skulle anonymiseras: hur skulle kommunen då kunna hjälpa och stödja den enskilde individen? Att anonymisering var en icke-fråga visade sig också i att ingen deltagare egentligen hade funderat på för- eller nackdelar med att anonymisera data innan de deltog i undersökningen.



Figur 10: Exempel på olika uttalanden om anonymisering från fokusgrupp-undersökningen.

I fokusgrupperna var många deltagare därför kluvna, eftersom kommunen inte kan sätta in resurser för en enskild individ om data anonymiseras. Men när diskussionerna hade pågått ett tag och deltagarna hade fått exempel på hur aggregerade anonymiserade samkörda data från olika förvaltningar skulle kunna vara till nytta för invånarna, blev fler deltagare mer välvilligt inställda till anonymisering, och resonerade att om data är anonym, ja då skulle de kunna dela hur mycket data som helst, då hade det inte spelat någon roll (se figur 10).

Vid diskussionerna i fokusgrupperna var deltagarna i slutänden överens om att frågan kring anonymisering (eller inte) fyller olika funktioner. Med individdata handlar det om nytta för just mig, den enskilde individen, vilket kan vara nödvändigt exempelvis vid en sjukdomshistoria för att kunna sätta in rätt resurser, medan aggregerade anonymiserade data kan vara värdefullt för många, för att kunna hitta mönster och sätta in åtgärder för specifika grupper eller områden inom kommunen.

Följaktligen, när frågan om anonymisering ställdes kopplat till något invånarna inte hade erfarenhet av, som samkörning, var det fler som tyckte att anonymisering var viktig (51 procent), än när invånarna tillfrågades om vad som gör att de känner sig tryggare med att dela data i allmänhet (21 procent tyckte då att anonymisering ökade tryggheten). Detta kan vara en konsekvens av att när man inte riktigt vet vad något innebär (som samkörning av stora datamängder) och har svårt att förstå konsekvenserna av det, kan det kännas tryggare att vara anonym.

Sammanfattningsvis visar detta på ett antal saker:

- Anonymisering av data är viktigt för tryggheten när man är osäker på hur data kommer att användas och av vem.

- Invånarna hyser stor tilltro till kommunens hantering och användning av deras data. Invånarna ställer sig i snarare frågande till hur data kan vara anonymiserad i relationen till kommunen: gör de verkligen nytta då?

- Som redan nämnts är det svårt att be användare ta ställning till ny teknik om de inte har kunskap om hur den fungerar och vilken konsekvens användningen av den kan få.

- Frågan om anonymisering är, om inte en icke-fråga, så i alla fall inte en speciellt viktig parameter när det kommer till helsingborgarnas upplevelse av trygghet i relation till kommunens (nuvarande och framtida) användning av deras data.

Medborgarinvolvering

Behovet av aktiva medborgare för att utveckla ny och hållbar samhällsservice tycks bli allt viktigare i samhällsutvecklingen. I de fem hypoteslabben där projektet Datalabbet ingick, var en utgångspunkt att invånarnas delaktighet är en stor potential för kommunens utveckling inom olika områden.

När man involverar personer i utvecklingen av framväxande tekniker och innovationer, det vill säga i fenomen som ännu inte existerar ens på prototypstadie, som i Datalabbet, är det som nämnts en utmaning att hitta en nivå på diskussionen som gynnar både deltagarna och de som utvecklar tekniken. I mötet med helt nya fenomen, är det svårt för deltagarna att ta ställning. I många fall vill man inte ha (eller vet inte om att man vill ha) radikala förändringar, utan bara något som är lite bättre än det som redan finns. Som jämförelse kan Henry Fords påstått (ö)kända citat – ”Om jag hade frågat vad människor ville ha skulle de ha svarat en snabbare häst” – användas. Citatet populariserades på 2000-talet av Apples Steve Jobs, när han skulle förklara varför Apple inte gör marknadsundersökningar och frågar användarna vad de vill (ha), innan de började tillverka sina innovativa tekniker. Det finns alltså en inställning att denna typ av diskussioner kanske inte ger de förslag eller djuplodande insikter som de som står för teknikutvecklingen anser sig behöva.

I nuläget ligger kommunens funderingar på hur man vill samköra data på en (för) abstrakt nivå som invånare inte riktigt förstår och kan ta ställning till. När kommunen kommer till steget att börja utveckla prototyper för nya tjänster kopplade till samkörning, blir det lättare för invånarna att rent konkret begripa hur tekniken kan påverkar dem, och kommer då också kunna bidra med insikter på ett mer konstruktivt sätt.

Med det sagt, är invånarnas åsikter även i nuläget viktiga. Men resultaten från den här studien handlar om att förstå invånarnas behov och attityder, till skillnad mot Datalabbets initiala syfte, som avsåg utveckla nya tjänster som bygger på samkörning. Dit har kommunen inte nått i ännu. Men resultaten från denna studie kan användas som grund för, och inspiration till, nya koncept och tjänster. I nästa steg kan liknande metodik användas för att gallra och validera bland koncept och prototyper, och därefter kan dessa testas för specifika situationer på olika målgrupper av invånare. Jämför man nuläget för kommunens arbete med samkörning och Fords fall, hade kanske önskemål

om snabbhet och större lastmöjligheter varit en återkoppling som gjort att Fords utvecklare kunnat jobba mer effektivt? Så även om kommunen och Datalabbet inte är riktigt är där man förväntade sig att vara resultatmässigt, har det varit viktigt att involvera invånarna så här långt. Invånarinvolvering är snarare en fråga om hur man lägger upp det man vill undersöka och vad man förväntar sig, än att det inte är någon idé att fråga vad människor vill och vill ha. Tillit i en demokrati handlar om utrymmet för människor att engagera sig och bli lyssnade på.

Figur 11: Inställning till och exempel på medborgarinvolvering i studiens undersökningar.

Förutom påståendena om kommunens digitaliseringsarbete, nådde undersökningarna i den här studien önskat antal deltagare och genererade positiv respons efter att de genomförts. Invånarna uppskattade möjligheten att vara med och påverka arbetet i kommunen (se figur 11). Påståenden som lades ut i kommunens sociala mediekanaler, som var ett oprövat sätt att försöka engagera invånare, genererade dock ovanligt få inlägg jämfört med hur det brukar vara på kommunens sociala medier, enligt den ansvariga för kanalerna. Därför är det viktigt att kommunens medborgarinvolvering sker på olika sätt. Det är inte självklart att alla sätt att involvera invånarna fungerar eller att alla vill vara med och påverka och engagera sig. Men om man inte kan nå dem som hyser låg tillit till kommunen och/eller andra grupper som är svårare att engagera, blir det mindre troligt att deltagande kan stärka tilliten i hela samhället. Därför är det viktigt att även nå kritiska medborgare. Låg tillit driver dock intresse för innovation och förändring. För ämnen som rör digitalisering kan denna grupp eventuellt vara lättare att involvera, än för andra ämnen.

Altruism

En ytterligare identifierad möjlighet är att i jämförelse med datadelning i kommersiellt syfte, tycks det finnas en altruistisk syn på datadelning i relation till kommunen. Invånarna såg nya kommunala datadrivna tjänster som ett sätt att förenkla och effektivisera vardagen för alla kommunens invånare. De menade också att sådana tjänster kan bidra till en bättre fördelning av kommunens resurser.

Även i fokusgrupperna fanns konsensus om att insamlade invånardata och datadrivna tjänster ska gynna lokalsamhället och invånarna i det, även om de också kan ha en egennytta. Deltagarna talade till exempel om ”våra data”, snarare än om ”mina data”. En bidragande faktor är sannolikt att invånarna hyser stor tillit till kommunen som datahanterare, vilket innebär att man har alla invånares bästa för ögonen (dvs, vertikal tillit). En annan orsak kan vara att ju mer aggregerade data blir, ju ”osynligare” blir den enskilda individen. Därmed minskar risken för integritetshot. Oavsett orsak, verkar inställningen vara att det finns ett demokratiskt värde av att dela data med och inom kommunen, att man som invånare i en kommun gynnas mer av att dela data, än att inte göra det. Detta kan jämföras med nationella studier som visar att majoriteten av internetanvändarna i Sverige inte delar data för att de vill, utan för att de anser att de måste för att kunna delta i det digitala samhället (Insight Intelligence 2020). Den altruistiska inställningen till datadelning med och inom kommunen är en bra förutsättning för kommunens fortsatta digitaliseringsarbete.

Sammanfattningsvis finnas det goda möjligheter för kommunen att utveckla och integrera användningen av ny teknik i nya tjänster, som inbegriper interaktiv samhällsstyrning där medborgaren har en medskapande roll.

Hot

Slutligen, det som identifieras som ett hot mot kommunens fortsatta digitaliseringsarbete är invånarnas **oro** för den ökande användningen av datahantering och datadrivna tjänster och beslut. Den här oron tar sig uttryck på olika sätt. Resultaten visar att invånarna framför allt oroar sig för:

- *Brister i upprätthållandet av den personliga integriteten.* Detta gäller kanske inte främst i interaktion med kommunen, utan delning av data generellt i samhället, och speciellt med vissa aktörer och för syften och tekniker man inte är tillräckligt insatt i. Men även vid datadelning med kommunen finns det ett behov av (mer) information om datadelningens syften, liksom ökade möjligheter för invånarna att kunna reglera vilka data man delar (se avsnitt ovan om transparens och behov av ökad kontroll).

- *Kunskapsbrist hos kommunen i att hantera utmaningar kopplad till ny teknik.* Invånarna litar på kommunen som organisation, men inte alltid på den enskilde tjänstepersonen. Om denne fattar felaktiga beslut, förväntas dock organisationen fånga upp detta. Men det finns en oro för att kommunen missar att tekniken gör fel, eller att kommunen börjar lita blint på tekniken och tror att den är ofelbar, och att invånarna därmed missgynnas. För att öka förutsättningarna för

kommunen att vara effektiv, rättssäker och korrekt, behövs bra kunskapsunderlag för datadrivna tjänster inom organisationen.

- *Bristande dataskydd och säkerhet.* Det finns en oro för att kommunen ska brista i sin säkerhet och att det kan leda till intrång där utomstående får tillgång till data och får möjlighet att missbruka dem. Säkerhet är en viktig komponent för tilliten till kommunen.

- *Avhumanisering i relationen med kommunen.* Det finns en oro för att all interaktion med kommunen ska komma att ske automatiserat, eller i alla fall enbart digitalt, utan möjlighet till fysisk eller mänsklig kontakt. Invånarna lyfte fram hur viktigt det är att kunna möta en människa, inte bara en maskin, vid kontakten med kommunen. Den personliga kontakten ansågs viktig dels för att man ska kunna förklara och få hjälp när beslut blivit fel, dels för behovet av mänsklig kontakt. Det kan därför vara viktigt att denna möjlighet finns kvar när kommunen utvecklar nya (digitala) sätt att interagera med invånarna, även om det inte är säkert att så många kommer att utnyttja den.

- *Att de digitala klyftorna ökar*. Här handlar det inte främst om en oro för att man själv ska missgynnas och automatiserade beslut och rekommendationer ska bli för individanpassade, utan en oro för att de digitala klyftorna ökar och att mindre hänsyn tas till människors olika situationer och olika behov av tjänster och kontakt med kommunen. Alla som betalar för kommunens tjänster har rätt att kunna ta del av dem, och att minimera digitala klyftor är en viktig uppgift i kommunens digitaliseringsarbete.

- *Oro för maskinella beslut:* Denna oro handlar till stor del om rädsla för det som är nytt och oprövat. Det kan innebära att när man inte vet att besluten sker automatiserat är man inte heller oroad av att använda en sådan tjänst. Exempelvis vet många svenskar inte att beslut om tillfällig föräldrapenning, inkomstbeskattning eller körkortstillstånd redan fattas av datorer (Denk m fl 2020), där bland andra Skatteverket är en av de myndigheter som har högst tillit hos svenskarna. Men det kan också innebära en oro över osäkerheten om hur besluten sker och att man inte har fått ta ett informerat beslut om hur man ställer sig till det. Ett viktigt arbete för kommunen är att minimera invånarnas oro för maskinella beslut.

Vilka är då mest oroliga? Det är invånare över femtio, personer med mindre tillit till andra människor, de som har mindre teknikvana, de som sällan besöker och använder Helsingborgs stads digitala kanaler samt de som inte är i kontakt med staden så ofta och inte känner till dess verksamheter så väl. Det är kanske inte helt oväntat att det är dessa grupper som känner störst oro. Samtidigt innebär det en utmaning för kommunens digitaliseringsarbete, eftersom det är just dessa grupper som kan vara svårare att nå ut till. Men det är naturligtvis viktigt för kommunen att på olika sätt adressera invånarnas oro, i det fortsatta digitaliseringsarbetet.

Sammanfattning

Invånarna i Helsingborgs stad ett högt förtroende för kommunens datahantering. Detta förtroende är naturligtvis viktigt att förvalta. Förtroendet grundar sig på den roll som kommunen anses ha: när kommunen agerar, gör den det i syfte att hjälpa invånarna och måna om deras bästa. Det gäller också datahantering, där kommunen antas och förväntas hantera data med kommuninvånarnas bästa för ögonen. Vidare ligger en viktig del av detta att kommunen följer de lagar och förordningar som finns och ser till att utomstående inte olovandes kan komma åt invånarnas data. Helst hade invånarna velat att även kommersiella aktörer skulle behöva följa det strikta(re) regelverk som kommunen med flera myndigheter behöver följa.

Samtidigt tror invånarna att kommunen redan använder mer dataanalys än vad de kan och gör idag, inklusive att samköra förvaltningsdata. Detta kan ses som motsägelsefullt. Men invånarna har generellt inte kunskap om vad kommunen juridiskt får göra och inte, och i tilliten till kommunen ligger en grundläggande förväntan om att kommunen agerar etiskt. Många uppfattar att kommunen tar ansvar för vad de får och inte får göra, inbegripet vad som är rätt och fel utifrån invånarnas perspektiv. Det finns också en förväntan på att kommunens agerande kommer leda till mer nytta för både invånare och samhälle, än om man låter bli att göra något, som exempelvis att samköra data. Vidare, förväntas det att kommunen tänker igenom och agerar efter vad det innebär att vara en ”bra” (eller ”god”) kommun. En grundbult för ett välfungerande samhälle med hög social tillit är myndigheters agerande som kan ses som förebilder för hur samhället ska skötas (Rothstein 2022).

Kommunens fortsatta digitaliseringsarbete bör grunda sig i detta etiska förhållningssätt. En viktig del av arbetet blir att stödja invånarnas kännedom och kunnande om digitaliseringens möjligheter och begränsningar. På så sätt kan de, både som individer och kollektiv, påverka digitaliseringen på ett för kommunen som helhet, gynnsamt sätt. För kommunen som organisation handlar det kommande arbetet om att fortsätta informera invånarna om existerande och nya möjligheter och förändringar och vid behov sätta in kunskapsinsatser riktade till specifika målgrupper, men också att förankra arbetet mer inom den egna organisationen. Det handlar också om att vara ännu tydligare med varför man samlar in invånarnas data och att ge konkreta exempel som invånarna kan relatera till. Vidare är det viktigt att fortsätta det innovativa arbete med framväxande teknik som påbörjats, exempelvis i Datalabbet, för att uppnå konkreta tjänster som kan komma kommunen till godo. En ytterligare aspekt är att utveckla möjligheterna att inkludera invånarna att vara delaktiga i utvecklingen, så att de upplever att de själva kan ta kontroll över både den och sina data. Sammantaget visar resultatet att det finns en god grund att stå på i kommunens fortsatta arbete. Fler studier behövs dock för att undersöka attityder till mer specifika tekniker och sammanhang.

I det här kapitlet har vi presenterat invånarna i Helsingborgs stads inställning till kommunens nuvarande och önskade dataanvändning och digitaliseringsarbete, specifikt det som rör AI-baserad samkörning av förvaltningarnas invånardata. Kommuninvånarnas inställning till delning, hantering och användning av persondata är dock inte den enda aspekten som påverkar kommunens digitaliseringsarbete. I nästa kapitel presenteras de juridiska utmaningar som finns för kommunen med stordataanalyser baserat på invånardata.

Referenser

Bylund, M. (2013). *Personlig integritet på nätet*. Stockholm: Fores.

Denk, T., Hedström, K. & Karlsson, F. (2019). Medborgarna och automatiserat beslutsfattande. I U. Andersson, B. Rönnerstrand, P. Öhberg & A. Bergström (red.), *Storm och stiltje*. Göteborg: SOM-institutet, 183–196.

Helsingborgs stad (2020). *Årsredovisning 2020*. Stadsledningsförvaltningen.

Holmberg, S. & Weibull, L. (2017). Långsiktiga förändringar i svenskt institutionsförtroende. I U. Andersson, J. Ohlsson, H. Oscarsson & M. Oskarson (red.), *Larmar och gör sig till.* Göteborg: SOM institutet, 39–57.

Insight Intelligence (2020). *Delade meningar: Svenska folkets attityder till digital integritet 2020.* Rapport. Insight Intelligence tillsammans med Karlstad universitet, Malmö universitet, Svensk Handel och Skatteverket.

Insight Intelligence (2021). *Delade meningar: svenska folkets attityder till digital integritet 2021.* Rapport. Insight Intelligence tillsammans med Skatteverket, Arbetsförmedlingen, Karlstads universitet och IAB Sverige.

Internetstiftelsen (2019). *Svenskarna och internet 2019*. Stockholm: Internetstiftelsen.

Kahneman, D. & Tversky, A. (1984). Choices, values and frames. *American Psychologist*, 39(4), 341-350.

Kruger, J. & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence leads to inflated self-assessments. *Journal of Personality and Social Psychology* 77(6), 1121–1134.

Larsson, S., Emanuelsson, T., & Thiringer, S. (2020). *Tillit eller tvång? Konsumenters förtroende för handelns datainsamling.* Stockholm: Fores.

Leckner, S. (2018a). Vem är positiv till insamling av användargenererade data på internet? I U. Andersson, A. Carlander, E. Lindgren & M. Oskarson (red.), *Sprickor i fasaden.* SOM-rapport nr 72. Göteborg: SOM-institutet, 55–70.

Leckner, S. (2018b). Sceptics and supporters of corporate use of behavioural data: Attitudes towards informational privacy and internet surveillance in Sweden. *Northern Lights*, 16(1), 113–132.

Malhotra, N., Kim, S. & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford: Stanford University Press.

Oscarsson, T. (2022). *Missnöjet har jäst sedan 2015*, Svenska Dagbladet 2022-12-17.

Regeringen (2018). Utgiftsområde 22: *Budgetpropositionen för 2019*. Prop. 2018/19:1.

Regeringen (2021). Utgiftsområde 22: *Kommunikationer*. Prop. 2021/22:1.

Riksrevisionen (2020). *Automatiserat beslutsfattande i statsförvaltningen – effektivt, men kontroll och uppföljning brister.* RiR 2020:20. Stockholm.

SOU (2016). *Hur står det till med den personliga integriteten? En kartläggning av Integritets-kommittén.* SOU 2016:41. Stockholm: Regeringskansliet.

Tillitsbarometern (2021). *Levande rapport 1: Tillitsbarometern*. Version 6. Stockholm: Ernsta Sköndal Bräcke högskola.

Trägårdh, L., Wallman Lundåsen, S., Wollebæk, D. & Svedberg, L. (2013). *Den svala svenska tilliten: förutsättningar och utmaningar.* Stockholm: SNS förlag.

Verbeek, P-P. & Tijink, D. (2020). *Guidance ethics approach: An ethical dialogue about technology with perspective on actions,* ECP.

Warren, M. E. (1999). *Democracy and trust*. Cambridge: Cambridge University Press.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

ETT JURIDISKT PERSPEKTIV PÅ DATADELNING:

Rättsliga ramar för datadelning i en kommun

Jonas Ledendal

Rättsliga ramar för datadelning

All offentlig verksamhet ska utövas med respekt för grundläggande fri- och rättigheter. 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 sina invånare. När en kommun hanterar uppgifter som rör kommunens invånare eller andra enskilda individer, måste kommunen följa tillämpliga bestämmelser om dataskydd och sekretess. I detta avsnitt ges en övergripande beskrivning av dataskyddsrättens grundläggande begrepp och de grundläggande krav (principer för dataskydd) som alltid måste vara uppfyllda när en myndighet behandlar personuppgifter.

Dataskydd

Rätten till privatliv och rätten till skydd av personuppgifter utgör grundläggande rättigheter enligt artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (EU-stadgan). Rätten till skydd av personuppgifter konkretiseras genom sekundärrättsakter, särskilt förordning (EU) 2016/679, den allmänna dataskyddsförordningen (GDPR). Syftet med den senare är att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter, men också att säkerställa att sådana uppgifter kan flöda fritt inom unionen (artikel 1 GDPR). Det fria flödet av personuppgifter säkerställs i första hand genom att alla EU-länder har enhetlig reglering av skyddet för personuppgifter. På så sätt kan inte de enskilda medlemsstaternas nationella rätt hindra överföringen av personuppgifter inom unionen. Det fria flödet av personuppgifter gäller även utbyte av personuppgifter mellan myndigheter om överföringen är nödvändig för att myndigheterna ska kunna utföra sina uppgifter (skäl 5 GDPR).

EU:s dataskyddsförordning, som började gälla den 25 maj 2018, är direkt tillämplig i Sverige och alla andra medlemsstater. Inom en förordnings eller annan rättsakts tillämpningsområde har denna företräde framför nationell rätt. Det innebär att en medlemsstat inte får införa nationella bestämmelser som strider mot unionsrätten. Nationella bestämmelser på dataskyddsrättens område får därför endast förekomma när det finns så kallade öppningsklausuler i förordningen. Exempel på en sådan öppningsklausul är artikel 85 GDPR, som gör det möjligt för en medlemsstat att sammanjämka yttrande- och informationsfriheten med bestämmelserna om dataskydd. I svensk rätt finns sådana bestämmelser i första hand i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). I denna anges bland annat när myndigheter får behandla känsliga personuppgifter. För den offentliga sektorn, bland annat delar av den kommunala förvaltningen, finns även ett stort antal specialförfattningar, till exempel lagen (2001:454) om behandling av personuppgifter inom socialtjänsten.

EU:s dataskyddsförordning har ett vidsträckt tillämpningsområde. Den omfattar alla de skiftande rättsordningar som finns i unionens medlemsstater och gäller dessutom inom helt olika verksamhetsområden (till exempel privat och offentlig sektor). Detta har lett till att bestämmelserna är förhållandevis abstrakt formulerade och inte sällan svåra att tolka i praktiken. Det finns dock

vägledning att hämta i rättspraxis från EU-domstolen (EUD). Det handlar dels om äldre praxis från det numera upphävda direktiv 95/46/EG (dataskyddsdirektivet), dels praxis som de senaste åren snabbt växt fram kring den nya dataskyddsförordningen. En sådan central fråga är hur begrepp som förekommer i GDPR ska tolkas när dessa inte har definierats i själva förordningen. Särskilda tolkningssvårigheter kan uppkomma när – som är vanligt – samma begrepp även finns i nationell rätt (till exempel ”myndighet” eller ”brott”). Här har domstolen slagit fast att när en rättsakt inte innehåller någon uttrycklig hänvisning till medlemsstaternas rättsordningar ska dessa normalt ges en självständig och enhetlig tolkning inom hela unionen (EUD mål C-439/19 Latvijas Republikas Saeima, punkt 81). Det går med andra ord inte att använda motsvarande begrepp från nationell rätt. I stället måste begreppen användas i den gemensamma betydelse som slagits fast i EU.

För att säkerställa en enhetlig tolkning och tillämpning har dessutom Europeiska dataskyddsstyrelsen (EDPB), befogenhet att utfärda riktlinjer, rekommendationer och bästa praxis (artikel 70 GDPR). Dessa rättsakter är visserligen inte bindande (artikel 288 FEUF), men har ändå stor praktisk betydelse för rättstillämpningen. Det finns också motsvarande uttalanden från Artikel 29-gruppen, som var EDPB:s föregångare. Sådana äldre uttalanden kan fortfarande vara relevanta för att tolka och tillämpa GDPR när det saknas nyare riktlinjer eller rättspraxis.

Tillämpningsområde

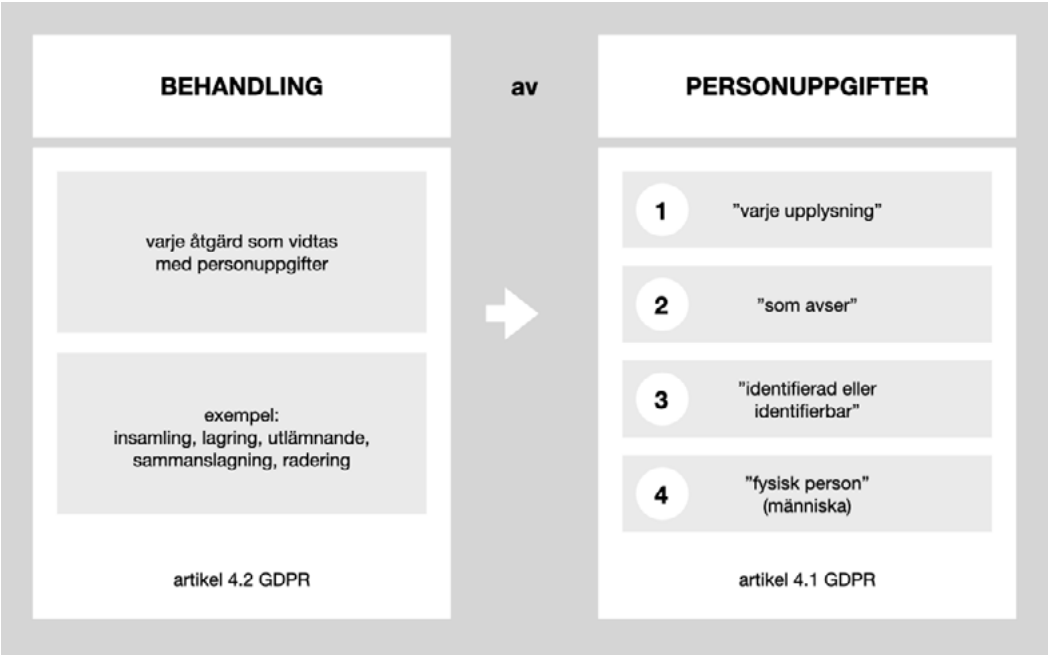
EU:s dataskyddsförordning gäller i princip vid all behandling av personuppgifter (artikel 2 GDPR). Dess tillämpningsområde bestäms av begreppen ”personuppgifter” och vad som ska anses utgöra ”behandling” av sådana uppgifter. Enligt EU-domstolen ska dessa begrepp ges en vidsträckt tolkning, vilket innebär att dataskyddsbestämmelserna får ett omfattande tillämpningsområde. Från detta tillämpningsområde görs endast vissa snävt avgränsade undantag som anges i förordningen.

Personuppgifter

Med ”personuppgifter” avses all slags information som rör en identifierad eller identifierbar fysisk person (artikel 4.1 GDPR). Förordningen skyddar alltså endast människor (fysiska personer), inte juridiska personer, såsom bolag, föreningar eller stiftelser (skäl 14 GDPR). Exempelvis kan en myndighet normalt utan hinder samla in och behandla uppgifter som rör ett bolag (till exempel firmanamn). Dessutom omfattas inte avlidna personer (skäl 27 GDPR). Svåra gränsdragningsfrågor kan dock uppkomma när en uppgift som avser en juridisk person, även kan sägas avse en fysisk person (till exempel ett företags ägare eller anställda) (EUD mål C-620/19 J & S Service). Samma gränsdragningsproblem uppkommer när en uppgift om någon som avlidit också kan anses röra en annan nu levande människa (till exempel en närstående). En och samma uppgift kan nämligen avse fler än en person (EUD mål C-434/16 Nowak).

För att något ska räknas som en personuppgift måste den som uppgiften avser (den registrerade) även vara identifierad eller identifierbar. Om den registrerade inte redan är identifierad måste det vara möjligt att direkt eller indirekt identifiera denne för att uppgiften ska räknas som en personuppgift. Det ska alltså åtminstone potentiellt vara möjligt att koppla uppgiften till en eller flera bestämda

personer. Med indirekt identifierbar aves att de medel som krävs för att identifiera en individ inte nödvändigtvis måste innehas av den som behandlar personuppgifterna (EUD mål C-582/14 Breyer). Det räcker att den senare med rimlig ansträngning till exempel kan förvärva de kompletterande uppgifterna eller de andra medel som krävs för att en identifiering ska vara möjlig (skäl 26 GDPR). En kommun kan till exempel ha uppgifter om någon som när dessa kombineras kan avslöja dennes identitet även om dessa uppgifter var för sig inte är identifierbara. När det inte är möjligt ska uppgifterna däremot betraktas som anonyma och omfattas då inte av dataskyddsförordningen (se vidare avsnitt om anonymisering).



Figur 1: Behandling av personuppgifter

Behandling av personuppgifter

Med ”behandling” av personuppgifter avses **varje åtgärd eller kombination av åtgärder** som vidtas med sådana uppgifter (artikel 4.2 GDPR). Det framgår av definitionen att förordningen gäller för hela datalivscykeln, det vill säga från att uppgifterna samlas in till att de raderas. Det räcker att uppgifterna lagras (till exempel på en hårddisk eller ett USB-minne) för att det ska räknas som en behandling. Det samma gäller för vidarebefordrande av uppgifter: även den som endast vidareförmedlar uppgifter (utan att förändra dessa) kan hållas ansvarig för att uppgifterna är riktiga och uppdaterade (EUD mål C-131/12 Google Spain och Google, punkt 29–31; mål C-73/07 Satakunnan Markkinapörssi

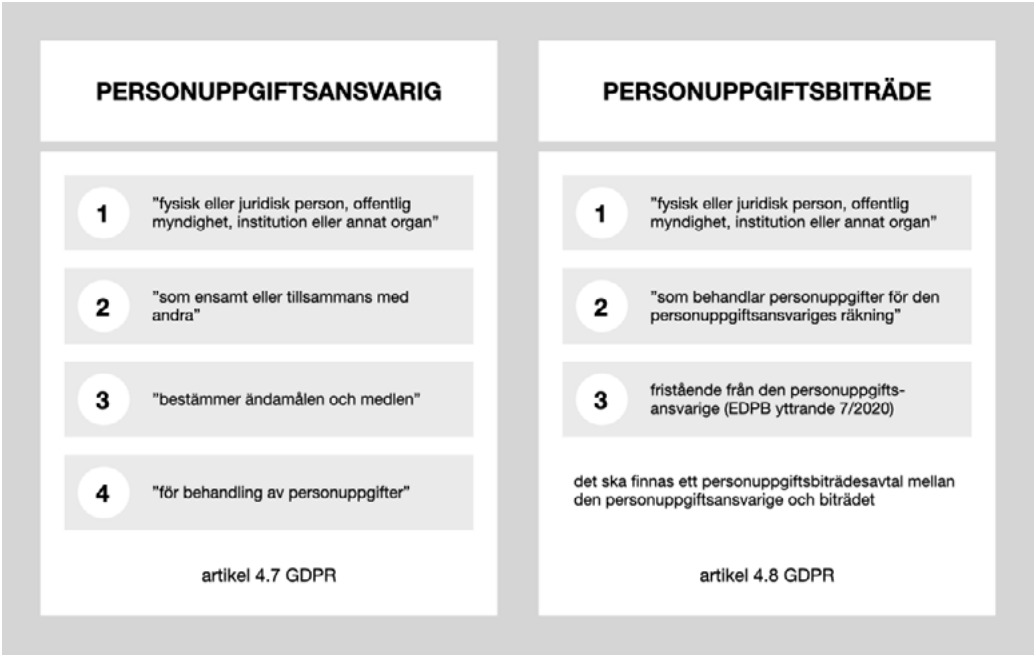
och Satamedia, punkt 48–49). Det räcker alltså med att en organisation innehar, eller på något annat sätt befattat sig med, personuppgifter för att dessa ska anses vara under behandling i dataskyddsrättslig mening. Det är heller inte nödvändigt att den personuppgiftsansvarige rent faktiskt har utfört behandlingen, eller ens haft tillgång till uppgifterna, för att räknas som ansvarig.

Dataskyddsförordningen är **teknikneutral** och är i princip tillämplig oavsett om behandlingen sker på automatisk eller manuell väg (skäl 15 GDPR). Det räcker att behandlingen i någon fas sker på automatisk väg (artikel 2.1 GDPR). Om behandlingen är fullständigt manuell gäller dock förordningen endast i begränsad omfattning. När uppgifterna behandlas på manuell väg, krävs att de ingår i eller kommer att ingå i ett register för att förordningen ska bli tillämplig (artikel 2.1 GDPR). Med ”register” avses att uppgifterna ingår i en strukturerad samling som är tillgänglig enligt särskilda kriterier (artikel 4.6 GDPR). Förordningen gäller alltså inte ostrukturerad information i pappersakter (skäl 15 GDPR). Enligt EU-domstolen räcker det dock att personuppgifterna strukturerats enligt kriterier som gör att dessa i praktiken och med lätthet kan tas fram och användas vid ett senare tillfälle (mål C-25/17 Jehovan Todistajat, punkt 61).

Enligt artikel 2.2 GDPR är vissa verksamhetsområden undantagna från förordningen. EU-domstolens fasta praxis säger dock att dessa undantag ska tolkas restriktivt. För det första finns det inget krav på att en verksamhet har något faktiskt samband med den fria rörligheten i det konkreta fallet (EUD de förenade målen C-465/00, C-138/01 och C-139/01 Österreichischer Rundfunk m.fl.). Det ska alltså inte göras någon kontroll av om den aktuella personuppgiftsbehandlingen har begränsat den fria rörligheten av varor, tjänster, personer eller kapital på den inre marknaden. För det andra, kan det undantag som föreskrivs i artikel 2.1 a GDPR (”verksamhet som inte omfattas av unionsrätten”), endast omfatta verksamhet som bedrivs av staten eller offentliga myndigheter (EUD mål C-101/01 Lindquist). Undantaget är dock inte automatiskt tillämpligt på all sådan verksamhet, utan det måste röra sig om nationell säkerhet eller verksamhet som (*ejusdem generis*) kan placeras i samma kategori (EUD mål C-272/19 Land Hessen, punkt 66–71). Det betyder att även om den verksamhet som bedrivs av kommunala myndigheter är av offentlig karaktär, kommer den kommunala organisationen till helt övervägande del att omfattas av unionens dataskyddsrätt. Det gäller även sådana kommunala verksamhetsområden som i strikt bemärkelse faller utanför unionsrättens tillämpningsområde (till exempel stora delar av socialtjänstens verksamhet).

Personuppgiftsansvar

EU:s dataskyddsförordning bygger på principen om **ansvarsskyldighet**. Detta innebär att det är den personuppgiftsansvarige som har det huvudsakliga ansvaret för att behandling av personuppgifter lever upp till de krav som föreskrivs i förordningen (artikel 5.2 GDPR). Det är denne som ska genomföra de **tekniska och organisatoriska skyddsåtgärder** som krävs för att dessa krav ska kunna uppfyllas (artikel 24 GDPR). Det räcker dock inte att åtgärder vidtas, den ansvarige måste också kunna visa att åtgärderna är lämpliga och leder till att behandlingen överensstämmer med förordningen. Den personuppgiftsansvarige har alltså **bevisbördan** för att behandlingen uppfyller de krav som ställs upp i artikel 5.1 GDPR (EUD mål C-175/20 Valsts ieņēmumu dienests, punkt 81).



Figur 2: Personuppgiftsansvarig och personuppgiftsbiträde

Personuppgiftsansvarig är den som har bestämt ändamålen och medlen för behandlingen (artikel 4.7 GDPR). Begreppet ska **tolkas funktionellt** enligt Europeiska dataskyddsstyrelsen. Detta innebär att det är den som faktiskt fattat detta beslut, snarare än den som hade den formella befogenheten, som är personuppgiftsansvarig (EDPB riktlinjer 7/2020, punkt 30). Den formella befogenheten utgör alltså endast en av flera omständigheter som ska beaktas för att fastställa vem som ansvarar för behandlingen. Det har till exempel inte någon avgörande betydelse hur parterna har reglerat detta ansvar i ett datadelningsavtal. Begreppet är **tvingande** och påverkas alltså inte av de beteckningar som parterna har valt att använda i avtalet (till exempel att en av dessa i egenskap av leverantör tar på sig rollen som personuppgiftsansvarig). För att en önskad ansvarsfördelning ska få avsedd rättsverkan måste denna även återspeglas av faktiska förhållanden.

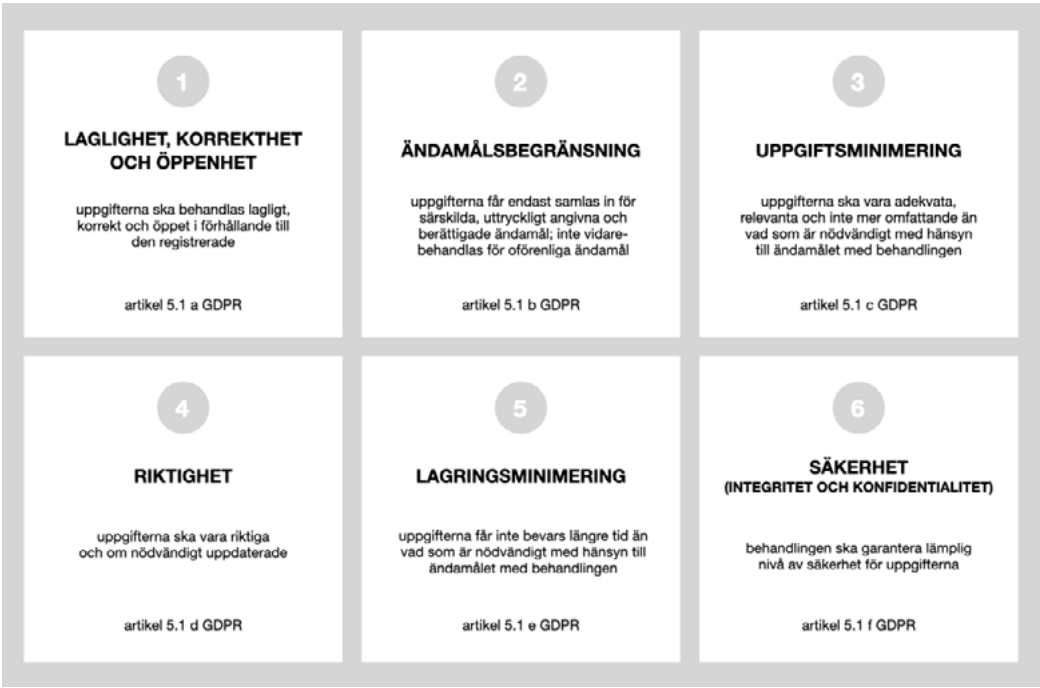
En myndighet kan vara personuppgiftsansvarig. I kommunal verksamhet är det normalt **kommunstyrelsen** eller de **kommunala nämnderna** som är personuppgiftsansvariga. Dessa utgör förvisso inte egna juridiska personer, men är att betrakta som myndigheter i statsrättslig bemärkelse (Strömberg & Lundell 2018). Även om detta formalistiska synsätt normalt har godtagits i svensk nationell rättspraxis, så är det värt att lägga märke till att dataskyddsförordningen inte ställer upp något krav på att den personuppgiftsansvarige ska vara en myndighet. EU-domstolen har slagit fast att definitionen av begreppet personuppgiftsansvarig är ”tillräckligt bred för att omfatta varje organ” (mål C-272/19 Land Hessen, punkt 65). Det finns till exempel inget hinder mot att ett parlamentariskt utskott i sig skulle kunna ses som personuppgiftsansvarig. Det innebär till exempel att en enskild skolenhet skulle kunna vara personuppgiftsansvarig, även om den enligt svensk nationell rätt bara utgör en osjälvständig del av den förvaltning som i sin tur är underställd den kommunala nämnd (myndighet) som ansvarar för skolan.

Personuppgiftsansvarig är den myndighet eller annat organ som faktiskt har haft ett bestämmande inflytande över ändamålen och medlen för behandlingen. Det är dock inte en nödvändig förutsättning att myndigheten eller organet själv har utfört behandlingen. Den personuppgiftsansvarige kan överlåta utförandet åt någon annan. När någon utför behandlingen för någon annans räkning, utan att själv ha utövat något inflytande över ändamålen och medlen, ska denne betraktas som **personuppgiftsbiträde** (artikel 4.8 GDPR). Ett sådant biträde kan vara en annan myndighet (till exempel Statens servicecenter) eller en kommersiell systemleverantör. När flera olika aktörer tillsammans har bestämt ändamål och medel för behandlingen kan dessa betraktas som **gemensamt personuppgiftsansvariga** (artikel 26 GDPR; artikel 4.7 GDPR). Alla de som deltagit i ett sådant gemenensamt beslut, måste dock inte ha ett lika långtgående ansvar (EUD mål C-40/17 Fashion ID, punkt 70). Exempelvis kan en utlämnande myndighet tänkas vara gemensamt ansvarig för överföringen men inte den vidare behandlingen.

En kommunal nämnd överlämnar dessutom normalt utförandet av behandlingen till förvaltningen och de tjänstepersoner som ska verkställa nämndens beslut. Den kommunala förvaltningen är en del av nämnden och utgör inte något självständigt kommunalt organ (se dock ovan angående EU-domstolens tolkning). Även om en fysisk person enligt förordningens definition (artikel 4.7 GDPR) kan vara personuppgiftsansvarig, betraktas normalt inte anställda (till exempel tjänstepersoner) som vare sig ensamt eller gemensamt personuppgiftsansvariga för behandling som utförs i tjänsten (EDPB riktlinjer 7/2020, punkt 19). Detta gäller även nämndens ledamöter. Detta förutsätter dock att personen endast behandlat personuppgifter på instruktion från arbetsgivaren (artikel 29 GDPR). Det är mindre klart vad som gäller om en tjänsteperson överträder förordningen genom att på eget initiativ behandla personuppgifter i strid med arbetsgivarens anvisningar (jfr. dock Kammarrättens i Stockholm dom 2022-11-07, mål nr 7678-21 där medarbetare vid Polismyndigheten olovligen använt programvara för ansiktsigenkänning i strid med arbetsgivarens riktlinjer, men myndigheten ändå ansågs vara personuppgiftsansvarig).

Principer för behandling av personuppgifter

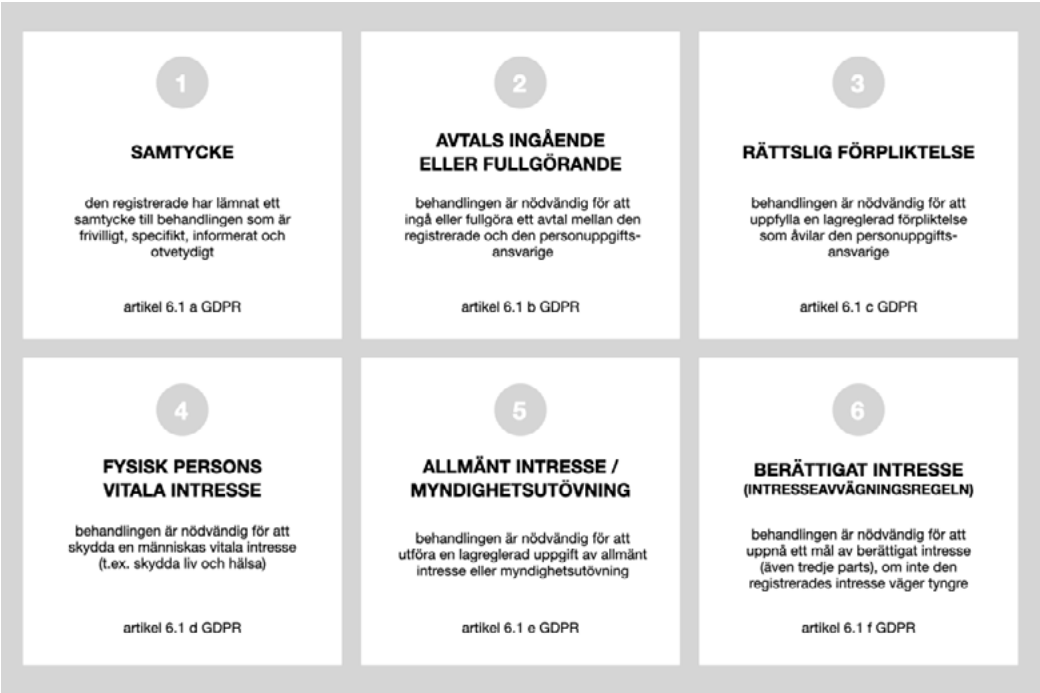
All behandling av personuppgifter måste överensstämma med de grundläggande principer för dataskydd som slås fast i artikel 5 GDPR (se figur 3). Principerna, som riktar sig till den personuppgiftsansvarige, gäller oavsett om behandlingen sker inom privat eller offentlig sektor. Även myndigheter ska alltså uppfylla de krav som anges i artikel 5. Medlemsstaterna har dock ett visst utrymme att begränsa dessa i den mån principerna motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22 GDPR (artikel 23 GDPR). Undantag kan också införas i nationell rätt med stöd av vissa andra öppningsklausuler i förordningen (till exempel artiklarna 85–88 GDPR). Exempelvis kan rätten att få personuppgifter rättade eller raderade begränsas när det från samhällssynpunkt finns ett intresse av att dessa ska bevaras för att tillgodose behovet av information för förvaltningen eller forskningens behov. Saknas sådana undantag i unionsrätten eller nationell rätt måste myndighetens delning av data uppfylla samtliga krav i artikel 5.



Figur 3: Principer för dataskydd

Laglighet

Artikel 5.1 a GDPR anger att personuppgifter alltid ska behandlas på ett lagligt sätt. Bestämmelsen genomför Artikel 8.2 i EU-stadgan, som föreskriver att personuppgifter ska behandlas ”på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund”. För att vara lagenlig måste behandlingen befinna sin inom ramen för de rättsliga grunder som anges i artikel 6.1 led a till f GDPR (se figur 4). Det är dock mindre klart om principen om laglighet även innebär att behandlingen måste ske i enlighet med alla andra bestämmelser i förordningen samt om principen också omfattar dataskyddsrättsliga bestämmelser i unionsrätten och en medlemsstats nationella rätt. En sådan vidsträckt tolkning skulle dock vara oförenlig med förordningens systematik. Att utsträcka kravet till all annan lagstiftning, skulle dessutom kunna komma i konflikt med unionsrättens princip om tilldelade befogenheter, som innebär att unionen och dess institutioner endast får vidta åtgärder inom de områden där de har tilldelats befogenhet att göra så av medlemsstaterna.



Figur 4: Rättsliga grunder för behandling av personuppgifter

I de förenade målen C-468/10 och C-469/10 ASNEF och FECEMD, slog EU-domstolen fast att den uppräkning av rättsgrunder som fanns i det gamla dataskyddsdirektivet var uttömmande. Det betyder att ”medlemsstaterna varken får foga ytterligare principer för tillåtligheten av behandlingen av personuppgifter till dem som nämns i artikel 7 i direktiv 95/46 eller föreskriva ytterligare villkor som påverkar räckvidden av de sex principer som föreskrivs i nämnda artikel” (punkt 32). Sedan dess har mål C-439/19 Latvijas Republikas Saeima (punkt 99), slagit fast att detta också gäller för de rättsliga grunderna i den nya dataskyddsförordningen. En medlemsstat kan dock göra vissa undantag från denna regel och själva närmare specificera vilka krav som ska vara uppfyllda för att behandlingen ska vara laglig. Enligt artikel 6.2 GDPR, kan medlemsstaterna till exempel behålla sektorsspecifik dataskyddslagstiftning inom den offentliga förvaltningen förutsatt att lagstiftningen är förenlig med förordningen.

En myndighet, eller annat offentligt organ, måste alltså grunda all sin behandling av personuppgifter på någon av de rättsgrunder som anges i artikel 6.1 GDPR (se figur 4 ovan). Det är dock viktigt att minnas att vissa av dessa rättsgrunder inte kan tillämpas av en myndighet. För det första, kan myndigheter normalt inte grunda sin behandling av personuppgifter på den registrerades samtycke. Anledningen till det är att det råder en så betydande ojämlikhet mellan en myndighet (den personuppgiftsansvarige) och den registrerade (till exempel en invånare eller brukare) att ett medgivande inte kan anses vara frivilligt (skäl 46 GDPR). För det andra, kan inte en myndighet grunda behandlingen på den så kallade intresseavvägningsregeln i artikel 6.1 f när den fullgör sina uppgifter (artikel 6.1 andra stycket GDPR). Det har nämligen varit unionslagstiftarens uppfattning att det är lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för myndigheters behandling av personuppgifter (skäl 47 GDPR). En myndighet kommer därför normalt att grunda sin behandling på antingen artikel 6.1 c (rättslig förpliktelse) eller artikel 6.1 e (allmänt intresse eller myndighetsutövning). Exempelvis kommer behandling av elevers personuppgifter normalt att grundas på skollagen eftersom det här endast finns ett begränsat utrymme för en kommunal skola att använda samtycke eller intresseavvägningsregeln.

Korrekthet (rättvisa)

Artikel 5.1 a GDPR anger att all behandling av personuppgifter ska vara korrekt (i svensk språkversion används omväxlande även ordet ”rättvis”). Bestämmelsen genomför artikel 8.2 i EU-stadgan, som föreskriver att sådana uppgifter ”must be processed fairly” (den svenska språkversionen av stadgan anger felaktigt att uppgifterna ska behandlas ”lagenligt”). Att varje behandling av personuppgifter måste vara både laglig och korrekt, utgör alltså en viktig grund för den rätt till skydd av personuppgifter som slås fast i artikel 8 i EU-stadgan. Kravet på behandlingens korrekthet/rättvisa har alltså ett särskilt starkt skydd. Av EU-domstolens rättspraxis framgår att principen inte bara har karaktär av målsättningsstadgande, utan utgör ett materiellt krav. Det är däremot inte helt klart vad kravet mer konkret innebär.

Europeiska dataskyddstyrelsen betraktar principen om korrekthet/rättvisa som en övergripande princip. Enligt principen får personuppgifter inte behandlas på ett sätt som är vilseledande, diskriminerande, överraskande eller till skada för den registrerade (EDPB riktlinjer 4/2019, punkt 69). Principen ställer också krav på att den personuppgiftsansvarige underlättar för den registrerade att utöva sina rättigheter. Enligt principen måste den personuppgiftsansvarige också beakta den registrerades (befogade) förväntningar, intressen och rättigheter. Behandlingen ska vid en sådan intresseavvägning inte vara oskälig i förhållande till den registrerade. Principen får därmed särskild relevans i en situation där det råder en betydande ojämlikhet (maktobalans) mellan den registrerade och den personuppgiftsansvarige (Holtz & Ledendal 2020).

En sådan maktobalans råder normalt mellan en myndighet och den enskilde (skäl 43 GDPR). När behandlingen, som normalt är fallet med myndigheter, grundas på en rättslig förpliktelse (artikel 6.1 c GDPR) eller uppgift av allmänt intresse (artikel 6.1 e GDPR) torde denna avvägning dock i första hand sammanfalla med den proportionalitetsbedömning som lagstiftaren ska göra enligt artikel 52.1 i EU-stadgan. Förutom att bedöma om en sådan nationell bestämmelse överensstämmer med stadgan är det alltså oklart om en myndighet ska göra en egen bedömning av om behandlingen är skälig i förhållande till den registrerade. Det myndigheten primärt ska bedöma är nämligen om den enskilda behandlingen har stöd i författning. Integritetsskyddsmyndigheten (IMY) har dock i vissa fall gjort en sådan separat bedömning av om behandlingen strider mot principen om korrekthet.

IMY har bland annat slagit fast att en kommuns kamerabevakning av en boendes sovrum på ett LSS-boende, var en så ingripande åtgärd att det inte kunde sägas leva upp till kravet på korrekthet (beslut 2020-11-24, dnr. DI-2019-7782). I ett annat tillsynsärende slog IMY fast att det stred mot principen om korrekthet att kameraövervaka de anställdas ombytesrum på en brandstation (beslut 2021-06-09, dnr. DI-2018-22697). Med hänsyn till att IMY i det senare fallet bedömde att den personuppgiftsansvarige haft rättslig grund för behandlingen enligt lagen om skydd om olyckor verkar myndigheten ha betraktat principerna om laglighet och korrekthet som separata krav. I båda fallen rör det sig dock om en proportionalitetsbedömning. Det hade därmed räckt för IMY att konstatera att en så ingripande kamerabevakning inte var nödvändig för att utföra den lagstadgade uppgiften och därmed saknade rättslig grund.

Öppenhet

Personuppgifter ska som utgångspunkt behandlas på ett öppet sätt i förhållande till den registrerade (artikel 5.1 a GDPR). Öppenhet är en förutsättning för att behandlingen ska kunna vara rättvis (se diskussionen om rättvisa ovan). Syftet med att ge den registrerade insyn i behandlingen är att denne ska kunna kontrollera om behandlingen har varit laglig. Kravet på öppenhet utgör med andra ord en nödvändig förutsättning för att den registrerade ska kunna utöva sina rättigheter, till exempel rätten till rättelse av felaktiga uppgifter eller rätten att invända mot behandlingen. EU-domstolen har därför särskilt betonat vikten av denna princip.

Tabell 1: Den personuppgiftsansvariges informationsskyldighet		
Information	**Direkt-insamling (artikel 13)**	**Tredjeparts-insamling (artikel 14)**
Personuppgiftsansvariges namn och kontaktuppgifter (samt eventuell företrädare i unionen)	•	•
Dataskyddsombudets kontaktuppgifter	•	•
Personuppgiftsbehandlingens ändamål och rättsliga grund	•	•
Om behandlingens grundas på samtycke, rätten att när som helst återkalla ett samtycke	•	•
Det berättigade intresse som behandlingen grundas på när denna sker enligt intresseavvägningsregeln	•	•
Kategorier av personuppgifter		•
Personuppgifternas källa		•
Om den registrerade enligt lag eller avtal är skyldig att tillhandahålla uppgifterna eller är nödvändigt för att ingå ett avtal samt möjliga följder av att inte uppgifter lämnas	•	
Mottagare eller kategorier av mottagare som kommer att ta del av uppgifterna	•	•
Överföring av personuppgifter till tredje land och om denna omfattas av beslut om adekvat skyddsnivå eller vilka lämpliga skyddsåtgärder som i stället vidtagits	•	•
Automatiserat beslutsfattande och profilering, meningsfull information om den bakomliggande logiken och dess följder	•	•
Lagringsperiod eller kriterier för hur den fastställs	•	•
Den registrerades rätt till tillgång, rättelse, radering, begränsning av eller att invända mot behandlingen, dataportabilitet	•	•
Rätt att klaga hos en tillsynsmyndighet	•	•

Öppenheten garanteras dels av att den personuppgiftsansvarige är skyldig att självmant lämna information, så kallad informationsskyldighet (artikel 13 och 14 GDPR), dels av den registrerades rätt att begära tillgång till sina uppgifter i form av ett registerutdrag (artikel 15 GDPR). Dataskyddsförordningen innehåller en uppräkning av vilken information som alltid ska lämnas till den registrerade. Vilken information som ska lämnas, skiljer sig åt beroende på om uppgifterna har samlats in direkt

från den registrerade eller om de samlats in från tredje part. Vilken information som ska lämnas i respektive fall framgår av **Tabell 1**. Den huvudsakliga skillnaden är att vid tredjepartsinsamling har den registrerade rätt att få veta vilka kategorier av uppgifter som behandlas och från vilka källor dessa uppgifter kommer.

Det är inte tillåtet att behandla personuppgifter utan att den registrerade på förhand har informerats. Vid direktinsamling ska den registrerade få den informationen denne har rätt till senast i anslutning till att uppgifterna samlas in (artikel 13.1 GDPR). När personuppgifterna erhållits från tredje part, ska den personuppgiftsansvarige i stället underrätta den registrerade i efterhand. Detta ska göras inom en rimlig period efter att uppgifterna har mottagits (artikel 14.3 GDPR). Tidsfristen ska bestämmas utifrån de särskilda omständigheter under vilka de aktuella personuppgifterna behandlas, men får inte överstiga en månad.

Det finns dock vissa undantag där den registrerade inte har rätt till information. Den personuppgiftsansvarige har till exempel aldrig någon skyldighet att lämna information som den registrerade redan förfogar över (artiklarna 13.4 och 14.5 a GDPR). När personuppgifterna kommer från tredje part behöver information inte heller lämnas i fall då: det skulle vara omöjligt eller kräva en oproportionerlig ansträngning; lagen kräver att personuppgifterna hämtas in eller då uppgifterna omfattas av yrkesmässig tystnadsplikt (artikel 14.5 b-d GDPR). Det kan till exempel innebära en oproportionerlig ansträngning att lämna information om det handlar om ett mycket stort antal registrerade (skäl 62 GDPR). Medlemsstaterna har också undantagsvis rätt att begränsa den registrerades rätt till information i nationell rätt (artikel 23 GDPR). Den registrerades rätt till information kan till exempel begränsas för att upprätthålla allmän säkerhet eller vid utredning av brott.

Ändamålsbegränsning

Principen om ändamålsbegränsning (även kallad finalitetsprincipen) betraktas som en av dataskyddsrättens hörnstenar (Kranenborg 2021). Principen, som lagfästs i artikel 5.1 b GDPR, består av två krav: (1) personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål (**ändamålsbestämning**), (2) dessa uppgifter får senare inte behandlas på ett sätt som är oförenligt med de ändamål för vilka de ursprungligen samlades in (**ändamålsbegränsning** i snäv bemärkelse). Syftet med principen är att undvika så kallad ändamålsglidning, det vill säga att personuppgifterna stegvis används för helt andra syften än vad den registrerade kunde förutsätta när uppgifterna samlades in. Det är med andra ord viktigt att alltid ange ändamålet med insamlingen av personuppgifter, annars har inte den registrerade möjlighet att ta ställning till om denne vill lämna sina uppgifter eller ej. Att ange ändamålet är också en förutsättning för att flera andra bestämmelser i förordningen ska kunna tillämpas. Dessa kräver nämligen inte sällan att en bedömning görs i förhållande till ändamålet med behandlingen.

Figur 5: Ändamålsbegränsning

Kravet på ändamålsbestämning innebär att den personuppgiftsansvarige alltid måste specificera ändamålet med behandlingen. Artikel 5.1 b GDPR genomför artikel 8.2 i EU-stadgan, som anger att personuppgifter endast får behandlas för ”bestämda ändamål”. Detta ska göras senast vid den tidpunkt då uppgifterna samlas in (skäl 39 GDPR). Förordningen kräver även att dessa ändamål är ”uttryckligt angivna”, vilket brukar tolkas som att dessa ska dokumenteras (de olika språkversionerna lämnar dock ett visst tolkningsutrymme). Den personuppgiftsansvarige måste under alla omständigheter kunna visa att kravet på ändamålsbestämning har uppfyllts (artikel 5.2 GDPR) och enligt principen om öppenhet ska information om ändamålet med behandlingen lämnas till den registrerade (artiklarna 13.1 c och 14.1 c GDPR). Ändamålet med behandlingen ska dessutom dokumenteras i den personuppgiftsansvariges register över behandling (artikel 30.1 b GDPR). Med berättigade ändamål avses, enligt EU-domstolen, att insamlingen har en rättslig grund (mål C-175/20 Valsts ieņēmumu dienests, para. 66).

När personuppgifterna väl har samlats in får de inte vidarebehandlas för några andra ändamål än de som angavs när uppgifterna först samlades in. Med vidarebehandling avses alla åtgärder som vidtas med uppgifterna efter att de har samlats in, inklusive registrering och lagring. Förordningen gör alltså skillnad mellan när personuppgifterna behandlas för samma eller olika ändamål. Om någon vill vidarebehandla personuppgifter, måste den personuppgiftsansvarige göra en bedömning av om den nya behandlingen (till exempel att lämna ut uppgifterna till tredje part) är förenlig med det ursprungliga ändamålet. Hur en sådan bedömning ska göras anges i artikel 6.4 GDPR. Om det nya ändamålet är förenligt med det gamla, krävs ingen ny rättslig grund (skäl 50 GDPR). Om det nya ändamålet inte är förenligt med det gamla, krävs antingen att den registrerade ger ett nytt samtycke eller att den vidare behandlingen är tillåten enligt unionsrätten eller en medlemsstats nationella rätt. För myndigheter innebär det att vidarebehandling som inte är förenligt med det ursprungliga ändamålet, normalt kräver stöd i lag eller annan författning (se ovan om rättslig grund).

Undantag görs dock för vidarebehandling som sker för **arkivändamål** av allmänt intresse, vetenskapliga och historiska **forskningsändamål** eller **statistiska ändamål**. För dessa ändamål antas nämligen att behandlingen är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in. Ett sådant antagande motiveras av att arkivering, forskning och sammanställning av statistik är former av behandling som den registrerade bör räkna med. En förutsättning för att detta undantag ska vara giltigt är att den personuppgiftsansvarige har vidtagit lämpliga skyddsåtgärder, till exempel genom att uppgifterna pseudonymiseras (artikel 89 GDPR). Det är också oklart om behandling som sker med stöd av en sådan presumtion ändå kräver en ny rättslig grund.

Uppgiftsminimering

De personuppgifter som samlas in ska vara adekvata, relevanta och inte behandlas i en större omfattning än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (artikel 5.1 c GDPR). Detta krav på uppgiftsminimering syftar till att **begränsa behandlingens omfång till vad som är nödvändigt och proportionerligt** i förhållande till de bestämda ändamål för vilka personuppgifterna har samlats in och behandlas (se diskussionen ovan om ändamålsbegränsning). Förutom att behandlingen som sådan (bortsett från när den grundas på samtycke) ska vara nödvändig för att uppfylla kravet på rättslig grund, måste den personuppgiftsansvarige enligt artikel 5.1 c även göra ett urval av personuppgifter för att säkerställa att denna kvantitativt begränsas till det minimum av uppgifter som krävs för att uppnå målet med behandlingen.

För varje steg i behandlingen måste den personuppgiftsansvarige göra en bedömning av om de uppgifter som behandlas är adekvata och relevanta. En uppgift är **adekvat** om den med hänsyn till art eller innehåll är lämplig för att uppnå ändamålet med behandlingen. Att behandla känsliga personuppgifter för ett trivialt syfte skulle strida mot artikel 5.1 c, eftersom de risker som uppkommer för den registrerade inte är proportionerliga i förhållande till ändamålet med behandlingen. Uppgifterna måste också vara **relevanta** i betydelsen att de kan bidra till att uppnå målet med behandlingen. Om uppgifterna inte behövs för att uppnå ett visst mål, är de inte relevanta och får inte samlas in och behandlas.

Principen om uppgiftsminimering begränsar också mängden personuppgifter. Dessa får **inte vara mer omfattande än vad som är nödvändigt** i förhållande till ändamålet med behandlingen. Om det går att uppnå målet med färre uppgifter, är det enligt artikel 5.1 c inte tillåtet att inkludera fler uppgifter eftersom det utsätter de registrerade för onödiga risker. Detsamma gäller för antalet registrerade som berörs av behandlingen. Dataskyddsförordningen kräver alltså att den personuppgiftsansvarige gör ett representativt urval. Principen om uppgiftsminimering är dock inte oförenlig med behandling av stora datamängder. Den personuppgiftsansvarige kan välja fritt mellan olika metoder för att behandla personuppgifter, men måste kunna visa att den valda metoden är proportionerlig i förhållande till ändamålet.

Lagringsminimering

Personuppgifter får enligt principen om **lagringsminimering** inte bevaras under längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas (artikel 5.1 e GDPR). För att uppfylla kravet på lagringsminimering måste en myndighet ange under vilka perioder uppgifterna kommer att lagras, eller åtminstone vilka kriterier som kommer användas för att fastställa dessa perioder (artikel 13.2 a eller 14.2 a GDPR). När uppgifterna inte längre behövs för dessa ändamål, ska de raderas eller avidentifieras (skäl 39 GDPR). Den personuppgiftsansvarige ansvarar för att detta kontrolleras regelbundet. Även här görs dock undantag för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål (se ovan om ändamålsbegränsning). Principen hindrar alltså inte att myndigheter arkiverar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. För att undantaget ska vara tillämpligt ställs dock samma krav på att myndigheten vidtar särskilda skyddsåtgärder enligt artikel 89.1 GDPR.

Riktighet

Personuppgifter ska vara riktiga och om nödvändigt uppdaterade (artikel 5.1 d GDPR). Att uppgifterna är riktiga och uppdaterade är särskilt viktigt om de ska användas som underlag för beslutsfattande. Felaktiga uppgifter kan dock också skada en persons anseende. Det är förvisso sant att en felaktig uppgift även kan vara till den registrerades fördel (till exempel att en arbetsgivare lämnat en för låg uppgift om inkomst), men den registrerade har ingen rätt att begära att sådana felaktiga personuppgifter ska bevaras. Det går inte heller att hävda att yttrande- och informationsfriheten ger någon rätt att sprida eller få tillgång till felaktig information (mål C-460/20 Google, punkt 65).
I vilken utsträckning denna rätt har företräde framför rätten till privatliv eller rätten till skydd av personuppgifter i EU-stadgan påverkas alltså av om de ifrågavarande uppgifterna är felaktiga.

En personuppgift kan vara oriktig på grund av att dess innehåll inte stämmer överens med verkliga förhållanden eller på grund av att den har blivit inaktuell. Detsamma gäller för en ofullständig uppgift, eftersom den kan ge en missvisande bild av den registrerade. Vad som utgör en felaktig personuppgift måste bedömas utifrån vilket ändamål den behandlas. Exempelvis är det inte lika viktigt att uppgiften är aktuell om den behandlas för arkivändamål eller historiska forskningsändamål.
I princip omfattas både faktauppgifter och värdeomdömen av kravet på riktighet. EU-domstolen har dock slagit fast att de ska bedömas olika eftersom det går att belägga sanningshalten i ett

faktapåstående, medan det inte går att bevisa riktigheten i ett värdeomdöme (mål C-460/20 Google, punkt 66).

Den registrerade har enligt artikel 16 GDPR, rätt att utan onödigt dröjsmål få felaktiga personuppgifter som rör denne rättade. Detta innefattar rätten att få komplettera ofullständiga personuppgifter (till exempel genom ett kompletterande utlåtande). Den personuppgiftsansvarige måste dock även utan en sådan begäran vidta alla rimliga åtgärder för att säkerställa att felaktiga personuppgifter rättas eller raderas utan dröjsmål (artikel 5.1 d GDPR). Detta gäller särskilt i samband med insamling och utlämnande. En myndighet är även skyldig att bedriva registervård och se till att de lagrade uppgifterna uppdateras så att de överensstämmer med den registrerades faktiska situation (EUD mål C-524/06 Huber, punkt 60). Samtidigt har EU-domstolen gjort åtskillnad mellan en begäran om rättelse och de krav som kan ställas på den personuppgiftsansvariges skyldighet att aktivt utreda om en personuppgift är felaktig (mål C-460/20 Google, punkt 67–77). I normala fall kan kravet om att rätta felaktiga personuppgifter uppfyllas genom att myndigheten har lämpliga rutiner för datainsamling (till exempel datakällor) och kvalitetskontroll.

Säkerhet för personuppgifter

Den som behandlar personuppgifter måste även kunna garantera en adekvat nivå av informationssäkerhet (artikel 5.1 f GDPR). Detta krav gäller under hela datalivscykeln, från insamling till radering av uppgifterna. Både personuppgiftsansvariga och personuppgiftsbiträden måste vidta de tekniska och organisatoriska åtgärder som är lämpliga för att uppnå en tillräcklig säkerhetsnivå (artikel 32 GDPR). Syftet med dessa säkerhetsåtgärder är att förhindra en personuppgiftsincident (artikel 4.12 GDPR), det vill säga att personuppgifterna oavsiktligt eller olagligt förstörs, ändras eller går förlorade, att personuppgifterna obehörigen röjs eller att någon obehörig får åtkomst till dem. Det rör sig alltså om åtgärder för att minska risken för en sådan incident (till exempel genom kryptering). Detta innefattar att bevara uppgifternas konfidentialitet (sekretess). Det innebär att en myndighet måste säkerställa att anställda och andra som utför arbete åt myndigheten, endast kan få tillgång till personuppgifter som denne behandlar på instruktion av den personuppgiftsansvarige (artikel 32.4 GDPR).

En personuppgiftsincident (till exempel ett dataintrång) innebär inte i sig att den personuppgiftsansvarige eller ett biträde gjort sig skyldig till en överträdelse av EU:s dataskyddsförordning. En incident räknas först som en överträdelse, om incidenten orsakats av en otillräcklig säkerhetsnivå. Det räknas också som en överträdelse om den ansvarige har mörklagt en incident. En incident ska utan onödigt dröjsmål, och senast inom 72 timmar, anmälas till behörig nationell tillsynsmyndighet (artikel 33 GDPR). För svenska myndigheter ska incidenter normalt anmälas till Integritetsskyddsmyndigheten (artikel 55 GDPR). Ett biträde ska skyndsamt underrätta den personuppgiftsansvarige (artikel 33.2 GDPR). När en incident sannolikt leder till en hög risk för fysiska personers grundläggande fri- och rättigheter, ska den personuppgiftsansvarige även utan onödigt dröjsmål underrätta de registrerade (artikel 34 GDPR). Europeiska dataskyddsstyrelsen har antagit riktlinjer om anmälan av personuppgiftsincident (EDPB riktlinjer 9/2022).

Insamling

Första steget i datalivscykeln utgörs av att data samlas in. Eftersom redan insamling av personuppgifter räknas som ”behandling”, måste den som ansvarar för insamlingen börja med att avgöra om insamlingen kommer att innefatta personuppgifter. Om så är fallet måste insamlingen leva upp till alla krav som föreskrivs i EU:s dataskyddsförordning samt kompletterande svensk nationell lagstiftning. I det här avsnittet diskuteras dels när något ska räknas som en ”insamling” av personuppgifter, dels vad som krävs för att en myndighet ska uppfylla kraven på ändamålsbestämning och rättslig grund i samband med att den samlar in sådana uppgifter.

Insamling av personuppgifter

Begreppet ”insamling” av personuppgifter förekommer på ett antal ställen i EU:s dataskyddsförordning, men definieras inte i förordningen. Det framgår dock av den uppräkning av behandlingsåtgärder som görs i artikel 4.2 GDPR, att redan insamling utgör en ”behandling” av personuppgifter. Det innebär att insamlingen som sådan måste ha en rättslig grund och leva upp till de krav som ställs i förordningen, särskilt de grundläggande principerna för behandling av personuppgifter som anges i artikel 5 GDPR. Det är alltså från och med denna tidpunkt som den personuppgiftsansvariges skyldighet att följa dataskyddsreglerna inleds. Det är dock viktigt att minas att flera av de tekniska och organisatoriska skyddsåtgärder som föreskrivs i förordningen, måste planeras och genomföras innan den faktiska insamlingen påbörjas.

Det är inte helt klart om personuppgiftsbegreppet i EU:s dataskyddsförordning avser konkreta exemplar av sådana uppgifter eller om detta tar sikte på deras abstrakta informationsinnehåll. Exempelvis inhämtas nya exemplar av uppgifterna varje gång en skola skickar ut en blankett för att samla in kontaktuppgifter till elevernas föräldrar, men om dessa inte ändrats erhåller skolan inte någon ny information. Om begreppet ska uppfattas som abstrakt får det alltså till följd att en ny insamling inte ska anses ha ägt rum om den personuppgiftsansvarige redan kände till uppgiftens innehåll medan denna omständighet saknar betydelse om begreppet i stället tar sikte på konkreta exemplar. Med ett konkret personuppgiftsbegrepp anses en ny insamling ha ägt rum även om det rör sig om dubbletter och förvärvet av dessa inte leder till att den ansvariga organisationen erhåller någon ny kännedom om förhållanden som rör den registrerade (t.ex. dennes namn eller ålder). Om begreppet är konkret eller abstrakt har också betydelse för om ett mångfaldigande av redan insamlade uppgifter i sig ska betraktas som en ny insamling. Eftersom de åtgärder som utgör en behandling enligt artikel 4.2 GDPR karaktäriseras av att de endast kan utföras på exemplar av uppgifter talar emellertid rättsystematiska skäl för ett konkret personuppgiftsbegrepp. Av det följer att det saknar betydelse om den ansvarige redan kände till eller förfogade över andra exemplar av uppgiften. Det räcker att ett nytt exemplar av en uppgift erhålls för att det ska vara att betrakta som en ny insamling.

Personuppgifter kan samlas in direkt från den registrerade (direktinsamling), men den personuppgiftsansvarige kan också helt lagenligt få tillgång till sådana uppgifter på något annat sätt. EU-domstolen har slagit fast att en insamling har ägt rum, oavsett om personuppgifterna kommer direkt från den registrerade eller efter begäran har tagits emot från tredje part (tredjepartsinsamling) (mål C-175/20 Valsts ieņēmumu dienests).

En fråga som varit omtvistad i rättslitteraturen är om en insamling i dataskyddsrättslig mening kräver eller inte kräver en aktiv handling från den personuppgiftsansvarige (Öman 2021, s. 124). Om det inte krävs en aktiv handling, skulle det innebära att någon kan bli ansvarig för uppgifter som denne passivt har mottagit utan att ha efterfrågat. Exempelvis skulle i så fall mottagaren göra sig skyldig till en överträdelse om någon skickat känsliga personuppgifter som mottagaren inte har rätt att samla in. För att förhindra att någon blir ansvarig för uppgifter som den inte bett om att få, har det i rättslitteraturen ansetts att den rimliga tolkningen är att ansvar inträder först om mottagaren aktivt gör något med uppgifterna (Arning & Rothkegel 2022 s. 122). För att undgå ansvar måste mottagaren också skyndsamt radera uppgifterna. När det gäller svenska myndigheter finns dock vissa nationella bestämmelser som beaktar att myndigheter har skyldighet att bevara inkomna handlingar enligt arkivreglerna.

Ändamålsbestämning

Senast i samband med att personuppgifterna samlas in måste den personuppgiftsansvariga myndigheten bestämma de särskilda ändamål som ska gälla för behandling av uppgifterna (artikel 5.1 b och skäl 39 GDPR). Hur dessa ändamål definieras påverkar hur uppgifterna får samlas in, men också hur dessa senare kan behandlas. Det gäller alltså att vara förutseende och redan på planeringsstadiet noga tänka igenom hur uppgifterna kan komma att behöva användas i framtiden. Bristfällig ändamålsbestämning kan nämligen leda till att sådan senare behandling blir otillåten.

Kravet på ändamålsbestämning i offentlig förvaltning

Ett bolag eller annat privaträttsligt subjekt har förhållandevis stor frihet att bestämma för vilka ändamål personuppgifter ska behandlas. Det är dock inte helt klart om denna frihet också gäller myndigheter. I motsats till företag och andra privaträttsliga subjekt, grundar sig en myndighets insamling nämligen normalt på lag eller annan författning. Det vanliga är att personuppgifterna samlas in för att myndigheten ska kunna utföra en lagstadgad uppgift, till exempel handläggning av ett ärende eller tillhandahållande av en välfärdstjänst (artikel 6.1 c eller e GDPR). Ändamålet med insamlingen bestäms då i första hand genom den lag eller annan författning som utgör rättslig grund för behandlingen. För myndigheter bestäms därmed ändamålet ofta av den rättsliga grunden för insamlingen.

När myndigheter behandlar personuppgifter, grundar sig alltså behandlingen normalt på en rättslig förpliktelse (artikel 6.1 c). En annan grund för myndigheter att samla in personuppgifter är att det utgör en uppgift av allmänt intresse (artikel 6.1 e). Det innebär att syftet i fråga om det förra ska fastställas direkt i den rättsliga grunden eller beträffande det senare vara nödvändig för att utföra

den ifrågavarande uppgiften (artikel 6.3 GDPR). Det räcker alltså inte att utförandet av en uppgift formellt har stöd i en författning. En sådan rättsgrund måste enligt EU-domstolens rättspraxis vara tillräckligt tydlig, precis och förutsägbar så att de enskilda individer som omfattas av åtgärden kan inrätta sig efter denna. Rättsgrunden måste också tydligt avgränsa dess tillämpningsområde och det sätt som befogenheten får utövas av behöriga myndigheter. En sådan rättsakt måste skydda enskilda mot godtyckliga ingrepp i deras grundläggande fri- och rättigheter, såsom deras rätt till privatliv. Inom den offentliga förvaltningen är kravet på ändamålsbestämning alltså nära förbundet med kravet på legalitet och rättssäkerhet.

Det är dock inte helt klart hur preciserat ändamålet måste vara och i litteraturen har konstaterats att de ändamål som framgår av lag många gånger är förhållandevis allmänt hållna i jämförelse med de krav som ställs upp för andra rättsgrunder, till exempel för att ett företag ska få behandla personuppgifter med den registrerades samtycke (von Grafenstein 2018 s. 295). Det har ibland motiverats med att det inte alltid är möjligt för lagstiftaren att på förhand ange för vilka särskilda ändamål de insamlade uppgifterna kan komma att användas.

För att avgöra om en bestämmelse (se exemplet med bibliotekslagen nedan) kan utgöra rättslig grund för en myndighets insamling av personuppgifter, är det nödvändigt att bedöma om behandlingens ändamål framgår tydligt för den registrerade. EU-domstolen har slagit fast att lagstiftningen måste begränsa myndigheternas användning av personuppgifter till ”bestämda, strängt begränsade syften som kan motivera det ingrepp som såväl åtkomst som användning av uppgifterna innebär” (mål C-362/14 Schrems, punkt 93). Det finns alltså ett nära samband mellan kravet på ändamålsbegränsning och kravet på proportionalitet. Vilka kriterier som ska användas för att bedöma om ändamålen är tillräckligt preciserade, framgår dock inte av vare sig dataskyddsförordningen eller domstolens praxis. En rättsgrund som tillåter att personuppgifter samlas in för obestämda ändamål eller ändamål som ännu inte är bestämbara måste dock anses vara oproportionerlig (von Grafenstein 2018 s. 281).

Ändamålsbestämmelser i kommunal speciallagstiftning

Ändamålsbestämmelser av olika slag förekommer också i en hel del av de specialförfattningar som reglerar behandling av personuppgifter i den offentliga förvaltningen. I lagen om behandling av personuppgifter inom socialtjänsten, finns inga entydiga regler för vilka personuppgifter som får samlas in. Definitionen av vad som avses med ”socialtjänst” (2 §), och kravet på att begränsa behandlingen av personuppgifter till vad som är nödvändigt för att utföra arbetsuppgifter inom detta område (6 §), innebär dock en tydlig begränsning av vilka ändamål som kan anses vara lagliga. Dessutom har regeringen fått rätt att föreskriva ytterligare begränsningar av när det är tillåtet att behandla personuppgifter inom socialtjänsten och när det inte är det (11 §). Att bestämma ändamålen direkt i lagen ansågs däremot utgöra ett alltför stort hinder vid verksamhetsförändringar (Prop. 2000/01:80 s. 142).

Några motsvarande bestämmelser finns inte på de verksamhetsområden som regleras av skollagen eller på biblioteksområdet. I skolan och på folkbiblioteket är det i stället skollagen eller bibliotekslagen som bestämmer vad som är ändamålsenlig behandling. Som påpekats ovan tenderar dock ändamålen i lagar som skollagen och bibliotekslagen ofta vara ganska allmänt beskrivna. Det gör det svårare att bedöma om dessa ändamål uppfyller kravet på att personuppgifter endast får samlas in för särskilda och uttryckligt angivna ändamål. Enligt 7 § bibliotekslagen definieras till exempel så övergripande ändamål som att folkbiblioteken ska främja läsning och tillgång till litteratur samt verka för att öka kunskapen om hur informationsteknik kan användas för kunskapsinhämtning, lärande och delaktighet i kulturlivet. Det finns en klar risk här att den vaga ändamålsbestämningen gör det svårt att verkligen säkerställa att behandlingen av personuppgifter blir tillräckligt förutsägbar.

EU-domstolen verkar medveten om problemet med vaga ändamålsbeskrivningar i nationell rätt. I mål C-175/20 Valsts ieņēmumu dienests hade domstolen att ta ställning till om dataskyddsförordningen utgjorde hinder mot att en skattemyndighet förelagt en leverantör av tjänster för publicering av annonser på internet att lämna ut uppgifter om skattskyldiga utan att syftet med begäran om utlämnande av uppgifterna var preciserat. Efter att ha konstaterat att behandlingen påbörjandes redan genom myndighetens begäran och att en sådan skulle räknas som ett led i insamlingen av personuppgifterna slog domstolen fast att när ett utlämnande inte direkt grundar sig på den rättsliga bestämmelse som utgjorde stöd för utlämnandet, utan följer av myndighetens begäran, måste det särskilda ändamålet i stället framgå av den senare för att det ska vara möjligt att kontrollera behandlingens lagenlighet (punkterna 60, 67 och 71).

Rättslig grund

För att behandling av personuppgifter ska vara tillåten, måste den grundas på den registrerades samtycke eller någon annan legitim och lagenlig grund. I EU:s dataskyddsförordning kommer denna princip till uttryck genom kravet på att behandlingen ska ha en rättslig grund (artikel 5.1 a; se även avsnittet ovan om principen om laglighet). Detta innebär att insamlingen, och alla andra åtgärder som vidtas med en personuppgift, ska grundas på någon av de sex rättsgrunder som räknas upp i artikel 6.1 GDPR (se figur 4 ovan). Förutom dessa sex rättsgrunder, måste myndigheter som vill samla in data också stödja all sin insamling och lagring av personuppgifter på någon av de rättsgrunder som finns i artikel 6.1 led a till f. Undantag görs endast för sådan myndighetsutövning som faller utanför förordningens tillämpningsområde (se dock ovan om förordningens vidsträckta tillämpningsområde).

Berättigade ändamål

Personuppgifter får enligt principen om ändamålsbegränsning endast samlas in för berättigade ändamål (artikel 5.1 b GDPR). Med detta menas att ändamålen måste kunna garantera en laglig behandling av personuppgifterna i den mening som avses i artikel 6.1 GDPR (EUD mål C-175/20 Valsts ieņēmumu dienests, punkt. 66). Det är dock inte helt klart om en sådan rättslig grund är det enda som krävs för att behandlingen ska vara berättigad enligt artikel 5.1 b GDPR. I sin senare rätts-

praxis har EU-domstolen indikerat att en rättslig grund endast är ett av flera krav som måste vara uppfyllda för att ändamålen ska kunna garantera en laglig behandling (mål C-77/21 Digi, punkt 27). Detta stämmer också överens med domstolens tolkning av kravet på laglighet i artikel 5.1 a GDPR, som även omfattar artiklarna 7–11 GDPR (mål C-60/22 Bundesrepublik Deutschland, punkt 58).

Kravet på att personuppgifter endast får samlas in för berättigade ändamål gäller även för myndigheter. För myndigheter kan detta påverka för vilka ändamål personuppgifter kan samlas in och behandlas. IMY har exempelvis funnit att personuppgifter som samlats in på en lärplattform, utan att plattformen hade en koppling till skolans verksamhet, inte hade samlats in för berättigade ändamål (beslut 2015-11-18, dnr. 2445-2014). Ett motsvarande synsätt har framförts av Socialdatautredningen som ansåg att endast ändamål som var nödvändiga för att utföra arbetsuppgifter inom socialtjänsten skulle betraktas som berättigade (SOU 1999:109). Dessa tolkningar överensstämmer, som framgår av ovan, med EU-domstolens rättspraxis. Med denna tolkning är en kommunal nämnd alltså förhindrad att samla in personuppgifter för ändamål som saknar koppling till de uppgifter som nämnden tilldelats genom lag eller annan författning.

Den registrerades samtycke

Det är normalt tillåtet att behandla någons personuppgifter om man först har inhämtat dennes samtycke (artikel 6.1 a GDPR). Att samtycke kan utgöra en legitim och lagenlig grund för behandling av sådana uppgifter framgår redan av artikel 8.2 EU-stadgan. Eftersom ett samtycke innebär att den registrerade avstår från en grundläggande fri- och rättighet, ställs höga krav på ett sådant samtycke. Även om detta gör att det ibland kan vara svårt, eller rent av omöjligt, att erhålla ett giltigt samtycke, så fungerar regeln om samtycke som en viktig säkerhetsventil som gör det möjligt att behandla personuppgifter i situationer när det annars hade varit otillåtet (Ledendal 2020). Samtycke kan till exempel användas när det saknas en annan rättslig grund. Under förutsättning att den personuppgiftsansvarige tillhandahållit fullständig information och medgivandet uppfyller de andra krav som ställs upp i förordningen, kan behandling grundad på samtycke ge en viss flexibilitet (för den personuppgiftsansvarige) samtidigt som en hög skyddsnivå bibehålls för den registrerades grundläggande fri- och rättigheter.

En myndighet kan dock endast i begränsad utsträckning använda samtycke som rättslig grund för behandling av personuppgifter. Ett sådant medgivande ska nämligen alltid vara frivilligt (artikel 4.11 GDPR). Den registrerade måste ha en äkta valmöjlighet, vilket inte är fallet när denne inte utan olägenhet kan avstå från att lämna eller återkalla ett samtycke (skäl 42 GDPR). När det gäller myndigheter anses den registrerades valmöjligheter vara begränsade, eftersom det råder en betydande ojämlikhet mellan det allmänna (den personuppgiftsansvarige) och den enskilde (den registrerade). Denna ojämlikhet gör det osannolikt att den registrerade har lämnat sitt samtycke frivilligt (skäl 43 GDPR).

Europeiska dataskyddsstyrelsen har dock uttalat att det inte är helt uteslutet att myndigheter kan använda samtycke som rättslig grund för behandling av personuppgifter enligt dataskyddsförordningen (EDPB riktlinjer 5/2020 punkt 16–20). En myndighet får dock inte villkora samtycket på ett sådant sätt att den registrerade inte får den information, den handläggning eller den tjänst som denne har rätt till om inte samtycke ges. Av riktlinjerna synes dock följa motsatsvis att samtycke kan användas för att tillhandahålla alternativa sätt att kommunicera med myndigheten som gör det enklare för den registrerade. Ett sådant utrymme verkar också finnas när myndigheten tillhandahåller vad som kan betecknas som tilläggstjänster vid sidan om de kärnuppgifter som myndigheten ska tillhandahålla enligt lag.

Det som avgör om en myndighet kan grunda behandlingen på samtycke eller inte, är om den registrerade har en äkta möjlighet att göra ett fritt val och utan olägenhet kan avstå från att samtycka eller återkalla medgivandet. Det är den personuppgiftsansvariga myndigheten som har bevisbördan för att en sådan äkta valmöjlighet har förelegat (artikel 7.1 GDPR). Exempelvis torde det normalt inte finnas något hinder mot att en kommunal skola använder elevers, eller när det rör sig om barn under tretton år deras vårdnadshavares, samtycke som grund för att framställa skolfoton/skolkataloger (artikel 8 GDPR och 2 kap. 4 § dataskyddslagen). Här rör det sig nämligen om frivillig verksamhet som ligger helt vid sidan av de uppgifter som kommunen har enligt skollagen. Även ett sådant samtycke ska så klart ges frivilligt (artikel 4.11 GDPR), men det finns ingen maktobalans som gör det motiverat att ställa högre krav än de som skulle ha gällt i privat sektor. Det är en annan sak om elever som inte deltagit i fotograferingen skulle förvägras utbildning, till exempel för att fotona också används för att identifiera eleverna i samband med examination (se EDPB riktlinjer 5/2020, punkt 20 för ett liknande exempel).

Berättigat intresse (intresseavvägningsregeln)

Enligt artikel 6.1 f GDPR kan personuppgiftsbehandling även vara tillåten utan den registrerades samtycke. Då måste dock den personuppgiftsansvarige kunna grunda behandlingen på ett berättigat intresse och vid en intresseavvägning måste det framgå att den registrerades intresse inte väger tyngre (den så kalladeintresseavvägningsregeln). Det måste också vara nödvändigt att samla in och behandla personuppgifter för att kunna uppnå det berättigade intresset. Det finns dock inget krav på att den personuppgiftsansvarige själv ska ha ett intresse av behandlingen. Det framgår av bestämmelsens ordalydelse att behandlingen lika väl kan grundas på tredje parts intresse. Det är därför som rättsgrunden normalt används vid utlämnande av personuppgifter till tredje part, till exempel i marknadsföringssyfte (Artikel 29-gruppen, yttrande 6/2014).

I samband med antagandet av GDPR föreslogs dock (KOM [2012] 11) ett nytt undantag som innebär att artikel 6.1 f GDPR inte ska gälla för myndigheter när de fullgör sina uppgifter (artikel 6.1 andra stycket). En sådan inskränkning gällde inte enligt det tidigare direktivet, vilket innebar att myndigheter kunde välja mellan om de till exempel skulle grunda behandlingen på artikel 6.1 led e (allmänt intresse) eller led f (berättigat intresse). En svensk myndighet kunde alltså från dataskyddsrättslig synpunkt tidigare välja att grunda sin behandling på 10 § f) personuppgiftslagen (1998:204)

(PUL) även om det saknades annat författningsstöd. En sådan ordning skulle dock strida mot flera andra medlemsstaters konstitutionella rätt och med övergången till en direkt tillämplig förordning framstår undantaget som en naturlig följd av kravet på att alla begränsningar av grundläggande fri- och rättigheter ska vara föreskrivna i lag. Att detta varit unionslagstiftarens syfte med undantaget framgår av ingressen som anger att då ”det är lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för de offentliga myndigheternas behandling av personuppgifter, bör [artikel 6.1 f] inte gälla den behandling de utför som ett led i fullgörandet av sina uppgifter” (skäl 47 GDPR).

Undantaget gäller dock endast när myndigheter ”fullgör sina uppgifter”, vilket som Artikel 29-gruppen konstaterat innebär att dess konsekvenser beror på om detta ska ges en restriktiv eller extensiv tolkning (yttrande 6/2014). Det är nämligen inte helt klart om artikel 6.1 andra stycket tar sikte på all verksamhet som bedrivs av en myndighet eller om undantaget endast omfattar uppgifter av allmänt intresse. EU-domstolen har dock numera slagit fast att undantaget ska tolkas på så sätt att artikel 6.1 led e och f utesluter varandra (mål C-180/21 Inspektor v Inspektorata kam Visshia sadeben savet, punkt 85). Det innebär att den personuppgiftsansvariga myndigheten först måste fastställa om dess behandling av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i dess myndighetsutövning på det sätt som avses i artikel 6.1 e GDPR (punkt 86). Om så är fallet omfattas behandlingen av undantaget och kan inte grundas på artikel 6.1 f GDPR.

Domstolens praxis slår alltså fast att en myndighet inte kan använda intresseavvägningsregeln vid myndighetsutövning (det vill säga utövandet av offentlig makt) eller när det rör sig om en uppgift av allmänt intresse. Undantagets räckvidd är alltså beroende av om ”uppgift av allmänt intresse” enligt artikel 6.1 e GDPR, ska ges en snäv eller vidsträckt innebörd. I det ovanstående målet slog domstolen fast att en åklagarmyndighet utförde en uppgift av allmänt intresse när den vidarebehandlade personuppgifter för att försvara staten mot en skadeståndstalan som grundade sig på fel i myndighetsutövning (mål C-180/21, punkterna 87–97). Domstolen verkar alltså öppen för att ”uppgift av allmänt intresse” även kan innefatta uppgifter som har ett tillräckligt nära samband med myndighetsutövning. Det saknades nämligen enligt domstolen ”betydelse att åklagarmyndigheten, i samband med en skadeståndstalan mot staten, agerar i egenskap av motpart på samma villkor som övriga parter och inte utövar myndighetsutövning” (punkt 90). Samtidigt slår domstolen fast att myndigheter kan använda artikel 6.1 f GDPR, när det inte rör sig om en uppgift av allmänt intresse eller myndighetsutövning.

Rättslig förpliktelse

När en myndighet samlar in och behandlar personuppgifter sker detta inte sällan för att myndigheten ska fullgöra en rättslig förpliktelse. Det kan till exempel röra sig om att myndigheten är skyldig att bedriva tillsyn. En sådan rättslig förpliktelse kan utgöra rättslig grund (artikel 6.1 c GDPR), men ska enligt Artikel 29-gruppens uppfattning ges en restriktiv tolkning (yttrande 6/2014 s. 19). För att denna grund ska bli tillämplig krävs att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. En sådan förpliktelse ska enligt 2 kap. 1 § data-

skyddslagen följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning (se vidare nedan om uppgift av allmänt intresse angående författningsstöd). Den personuppgiftsansvarige får inte ha en valfrihet. När en sådan skyldighet inte föreligger, får myndigheten alltså inte grunda behandlingen på artikel 6.1 c. När behandlingen har stöd i lag eller annan författning får denna i stället grundas på artikel 6.1 e GDPR (uppgift av allmänt intresse eller myndighetsutövning). Detta beror bland annat på att den registrerade hamnar i en mindre fördelaktig situation när dennes personuppgifter behandlas enligt led c i stället för led e. Exempelvis har den registrerade i det senare fallet rätt att invända mot behandlingen (artikel 21 GDPR).

I mål C-496/17 Deutsche Post. har EU-domstolen uttalat att en tullmyndighets insamling av personuppgifter för att kunna fatta beslut avseende en ansökan om status som godkänd ekonomisk aktör i enlighet med unionens tullkodex framstod som nödvändig för att fullgöra en rättslig förpliktelse (punkt 61–62). När syftet med behandling av personuppgifter är att göra det möjligt för en myndighet att handlägga en ansökan kan behandlingen alltså grundas på artikel 6.1 c. En sådan behandling kan dock många gånger även grundas på artikel 6.1 e GDPR eftersom den normalt utgör ett led i myndighetsutövning. Artikel 29-gruppen har framhållit att behandling som ligger nära artikel 6.1 c, men som inte fullt ut uppfyller de villkor som gäller för den rättsgrunden, i stället kan vara tillåten efter en intresseavvägning enligt artikel 6.1 f under förutsättning att det rör sig om ett berättigat intresse (yttrande 6/2014 s. 21).

Uppgift av allmänt intresse eller myndighetsutövning

Personuppgifter får enligt artikel 6.1 e GDPR behandlas när ”behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning”. Det är, som framgått ovan, unionslagstiftarens uppfattning att det i huvudsak är denna rättsgrund som ska användas vid myndigheters behandling av personuppgifter. Det är därför myndigheters behandling inte längre kan grundas på intresseavvägningsregeln.

Den svenska språkversionen lämnar öppet för olika tolkningar av några av de villkor som ingår i artikel 6.1 e GDPR. Det framgår exempelvis inte av ordalydelsen om nödvändighetskravet även gäller vid myndighetsutövning, eller endast när den rättsliga grunden vilar på ett allmänt intresse. I den svenska ordalydelsen framgår heller inte om bestämmelsen förutsätter att befogenheten att utföra den aktuella uppgiften ska ha tilldelats den personuppgiftsansvarige eller om ett krav på ett sådant samband endast ställs vid myndighetsutövning. Vid en jämförelse med andra språkversioner framgår dock att led e bör tolkas på så sätt att grunden är tillämplig när ”behandlingen är nödvändig för att utföra en uppgift”, som antingen är av ”allmänt intresse” eller innefattar ”myndighetsutövning” samt att utförandet av uppgiften ska ankomma på den personuppgiftsansvarige.

Rättsgrunden kan alltså användas när det rör sig om utförandet av en uppgift som är av allmänt intresse eller när en uppgift innefattar myndighetsutövning. Begreppet ”allmänt intresse” är ett självständigt unionsrättsligt begrepp, men medlemsstaterna har ett förhållningsvis stort tolkningsut-

rymme här. En jämförelse kan göras med begreppet ”tjänster av allmänt intresse”, som förekommer både i Funktionsfördraget och Protokoll 26 rörande tjänster av allmänt intresse. Någon definition av ”tjänster av allmänt intresse” finns inte i unionsrätten. Rättspraxisen visar dock att ”tjänster av allmänt intresse” kan röra både ekonomiska och icke-ekonomiska tjänster som medlemsstaterna anser vara av allmänt intresse och som staten därmed har vissa skyldigheter att tillhandahålla (Madell 2011). När unionsrättsliga regler saknas är det upp till varje medlemsstat att bestämma hur dessa ska organiseras, tillhandahållas och finansieras. Detta gäller särskilt tjänster av icke ekonomisk art eftersom dessa inte omfattas av unionens konkurrensregler.

Eftersom det saknas en definition i EU-lagstiftningen, är det medlemsstaterna som slår fast vad som är en uppgift av allmänt intresse enligt artikel 6.1 e GDPR i den nationella rätten. Det följer dock redan av ingressen till förordningen att vissa uppgifter ska anses vara av allmänt intresse. Hit hör hälso- och sjukvård, folkhälsa och socialt skydd. I det sociala skyddet ingår ersättningar som pensioner, arbetslöshetsersättningar samt sociala förmåner. Det framgår också av förordningen att arkivverksamhet kan vara av allmänt intresse. Dessa exempel visar att begreppet täcker in många av de skatte- eller avgiftsfinansierade välfärdstjänster som tillhandahålls av stat och kommun. Detta gäller utan tvivel de välfärdstjänster som kommuner är skyldiga att tillhandahålla, såsom förskola och skolbarnomsorg, grund- och gymnasieskola, särskola, kommunal vuxenutbildning, svenska för invandrare, socialtjänst, omsorg om äldre och funktionsnedsatta, stadsplanering, hälso- och miljöskydd, renhållning och avfallshantering, räddningstjänst, vatten och avlopp, bibliotek, krisberedskap och kollektivtrafik.

Begreppet ”myndighetsutövning” är heller inte definierat i dataskyddsförordningen, men även här torde det röra sig om ett självständigt unionsrättsligt begrepp. I unionsrätten används begreppet i första hand för att skilja mellan ekonomisk verksamhet och verksamhet som är förenad med utövandet av offentlig makt. Exempelvis omfattar förbudet mot inskränkningar i den fria etableringsrätten inte verksamhet som hos en medlemsstat är förenad med utövandet av offentlig makt. När det i dataskyddsförordningen anges att en uppgift ska utgöra ett led i den personuppgiftsansvariges myndighetsutövning, är avsikten på samma sätt att skilja mellan å ena sidan sådan ekonomisk verksamhet där unionslagstiftaren haft för avsikt att åstadkomma en enhetlig reglering och å andra sidan verksamhet som innefattar utövandet av offentlig makt där ett större handlingsutrymme har lämnats till medlemsstaterna. Begreppet torde sammanfalla med vad som i svensk rätt ska betraktas som handläggning av förvaltningsärenden, men kan även tänkas innefatta andra åtgärder som är förenade med utövandet av offentlig makt.

Med hänsyn till att villkoren ”allmänt intresse” och ”myndighetsutövning” är alternativa borde artikel 6.1 e GDPR i princip kunna tillämpas inom stora delar av den offentliga förvaltningen. Dessa begrepp får dessutom till viss del anses överlappa varandra. Att tillhandahålla tjänster av allmänt intresse innebär ju inte sällan att åtminstone den enskildes rätt fastställs genom ett myndighetsbeslut. Att det i förvaltningsrätten finns anledning att göra skillnad mellan beslut om försörjningsstöd (handläggning av ett förvaltningsärende) och utbetalning av detsamma (verkställighet), hindrar

inte att myndigheten i båda dessa avseenden behandlar den sökandes personuppgifter med stöd av artikel 6.1 e GDPR. Även om utövandet av offentlig makt i de allra flesta fall sker som ett led i utförandet av uppgifter som har ett allmänt intresse, kan det dock undantagsvis vara så att myndighetsutövning sker utan att det tjänar ett allmänintresse. Exempelvis innefattar användande av tvångsmedel i civilrättsliga tvister utövande av offentlig makt utan att det i strikt mening alltid finns ett klart allmänintresse. Även i de fallen bör dock led e kunna användas som rättsgrund.

Det är i sammanhanget också värt att påpeka att den rättsgrund som föreskrivs i artikel 6.1 e GDPR inte är förbehållen myndigheter och andra offentliga organ. Grunden kan alltså användas även om en kommun har valt att en tjänst av allmänt intresse ska tillhandahållas genom ett kommunalt bolag eller någon annan privaträttslig associationsform. När det gäller tjänster av allmänt intresse torde det heller inte vara något hinder att verksamheten bedrivs i vinstsyfte av ett privat företag. Exempelvis bör de uppgifter som utförs av skolor omfattas av artikel 6.1 e oberoende av om skolan har en kommunal eller privat huvudman. Detsamma gäller myndighetsutövning, som enligt svensk rätt kan överlämnas till andra juridiska personer (än kommuner) och fysiska personer förutsatt att det sker med stöd av lag. Vilken rättslig form som den personuppgiftsansvarige har saknar alltså betydelse, det avgörande är verksamhetens art.

Det är dock inte tillräckligt att konstatera att behandlingen sker som ett led i utförandet av en sådan uppgift som anges i artikel 6.1 e GDPR. Behandlingen av de ifrågavarande personuppgifterna måste även vara ”nödvändig” för utförandet av uppgiften. En behandlingsåtgärd ska enligt EU-domstolens rättspraxis vara strikt nödvändig och proportionerlig (se även nedan). Detta innebär att en åtgärd inte ska anses vara nödvändig så länge uppgiften kan fullgöras på ett sätt som medför ett mindre ingrepp i den registrerades grundläggande fri- och rättigheter. När det exempelvis gäller behandling för statistiskt ändamål har behandlingen inte ansetts nödvändig när det hade räckt att behandla anonyma uppgifter. Samtidigt har domstolen i mål C-524/06 Huber funnit att en behandlingsmetod ska anses nödvändig ”om den bidrar till att effektivisera tillämpningen av bestämmelser” i en viss lagstiftning. I målet ansågs det befogat att av effektivitetsskäl inrätta ett centralt nationellt register även om samma uppgifter kunde hämtas från kommunala befolkningsregister.

Det framgår dock av artikel 6.3 GDPR att utförandet av de uppgifter som anges i artikel 6.1 e ska ha fastställts i unionsrätten eller en medlemsstats nationella rätt. I artikel 6.3 och ingressen finns även en påminnelse om att varje begränsning av de grundläggande fri- och rättigheter som föreskrivs i EU-stadgan ska uppfylla vissa krav. I likhet med vad som anges i artikel 6.3 ska varje sådan begränsning vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa fri- och rättigheter. När det gäller dataskyddsförordningen framgår det av ingressen till denna att det inte nödvändigtvis måste röra sig om en lagstiftningsakt som antagits av ett parlament. Förutsatt att det är förenligt med en medlemsstats konstitutionella ordning kan en sådan bestämmelse alltså antas av något annat offentligt organ. Det räcker dock inte att utförandet av en uppgift formellt har stöd i en författning. En sådan rättslig grund måste vara tillräckligt tydlig, precis och förutsägbar så att de enskilda individer som omfattas av åtgärden kan inrätta sig efter denna. Den måste också

tydligt avgränsa dess tillämpningsområde och det sätt som befogenheten får utövas av behöriga myndigheter. En sådan lag måste skydda enskilda mot godtyckliga ingrepp i deras grundläggande fri- och rättigheter, såsom deras rätt till privatliv.

En sådan rättsgrund ska dessutom med beaktande av proportionalitetsprincipen vara nödvändig och faktiskt svara mot ett mål av allmänt samhällsintresse som erkänns i unionsrätten. Med det senare avses enligt EU-domstolens rättspraxis att begränsningen ska vara strikt nödvändig. Även om en åtgärd ska anses uppfylla detta krav måste den också vara proportionerlig i den meningen att de fördelar som begränsningen ger upphov till väger tyngre än de nackdelar som denna innebär för den enskildes möjlighet att utöva sina fri- och rättigheter. För att minska riskerna för den registrerades integritet är det viktigt att en sådan rättsakt innehåller lämpliga skyddsåtgärder. Exempelvis slog EU-domstolen i de förenade målen C-203/15 och C-698/15 Tele2 Sverige fast att den svenska lagstiftningen om datalagring gick utöver vad som var strikt nödvändigt i förhållande till det i och för sig berättigade målet att bekämpa allvarlig brottslighet.

I 2 kap. 2 § dataskyddslagen anges att personuppgifter får behandlas med stöd av artikel 6.1 e i EU:s dataskyddsförordning, om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning. Detsamma gäller när behandlingen sker som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning. Mot bakgrund av vad som sagts ovan om de krav som ställs upp i artikel 6.3 GDPR och motsvarande bestämmelser i EU-stadgan kan den ifrågavarande bestämmelsen i dataskyddsalgen inte i sig utgöra en rättslig grund som gör att behandling av personuppgifter är tillåten enligt unionsrätten. Den får i stället ses som en upplysning om var en sådan grund kan finnas i den svenska rättsordningen. För att kunna fungera som rättslig grund måste dessa föreskrifter i sin tur uppfylla de krav som anges i artikel 6.3 och EU-stadgan.

Känsliga personuppgifter

Behandling av känsliga personuppgifter är som huvudregel förbjudet enligt artikel 9.1 i EU:s dataskyddsförordning. Förbudet motiveras av att personuppgifter som räknas som känsliga till sin natur medför särskilda risker för den registrerades grundläggande fri- och rättigheter (skäl 51 GDPR). Detta gäller inte bara individens rätt till privatliv, bestämmelsen avser även att förstärka det skydd som redan finns mot olika former av diskriminering i artikel 21 i EU-stadgan.

Begreppet ”känsliga personuppgifter” förekommer inte i förordningen, men definieras i 3 kap. 1 § dataskyddslagen. Vilka uppgifter som ska räknas som känsliga, räknas upp i artikel 9.1 GDPR. Här definieras känsliga personuppgifter som:

> *personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.*

En del av dessa kategorier beskrivs närmare i artikel 4.13-15 GDPR, men annars har unionslagstiftaren lämnat mycket liten vägledning kring hur övriga kategorier ska tolkas. EU-domstolen har dock slagit fast att dessa ska ges en förhållandevis vidsträckt tolkning, vilket innebär att förbudet även ska tillämpas på uppgifter som indirekt kan avslöja känslig information om en fysisk person (EUD mål C-184/20 Vyriausioji tarnybinės etikos komisija, punkt 127).

För att det ska vara tillåtet att behandla känsliga personuppgifter måste behandlingen, förutom att ha en rättslig grund enligt artikel 6, även omfattas av något av de undantag som anges i artikel 9.2 GDPR. Exempelvid med stöd av den registrerades uttryckliga samtycke (artikel 9.1 a). I likhet med vad som gäller enligt artikel 6.1 a, får myndigheters möjlighet att grunda behandling av känsliga personuppgifter på ett sådant samtycke anses vara starkt begränsat. Åtminstone när det gäller behandling som innefattar utövandet av offentlig makt, måste myndigheter och andra offentliga organ förlita sig på något annat undantag. För handläggning inom socialtjänsten kan undantaget i artikel 9.2 b (social trygghet och socialt skydd) bli tillämpligt. Även om led b kan användas av myndigheter torde undantaget primärt rikta sig till den privata sektorn, såsom arbetsgivare och arbetstagarorganisationer (se nedan angående socialtjänstens möjlighet att grunda sin behandling på artikel 9.2 h GDPR).

I förordningen föreskrivs även att behandling av känsliga personuppgifter ska vara tillåten när detta är nödvändigt med hänsyn till ett viktigt allmänt intresse (artikel 9.2 g). Undantaget motsvarar den rättsliga grund som föreskrivs i artikel 6.1 e. I båda fallen ska behandlingen gälla ett allmänt intresse som har slagits fast i unionsrätten eller en medlemsstats nationella rätt. Den huvudsakliga skillnaden är att behandling av känsliga personuppgifter endast är tillåtet när det rör sig om ett viktigt allmänt intresse. Det kan till exempel handla om viktiga allmänintressen inom hälso- och sjukvårdens område, social omsorg respektive folkhälsoområdet (artikel 9.2 led h och i), där känsliga personuppgifter kan behöva delas för att kunna erbjuda dessa tjänster. Även undantaget som berör social trygghet och socialt skydd (se ovan) verkar motiveras av ett sådant starkt allmänintresse.

Gemensamt för att dessa undantag ska vara tillämpliga är att det, förutom stöd i unionsrätten eller en medlemsstats nationella rätt, även krävs att dessa föreskrifter innehåller lämpliga skyddsåtgärder som ska säkerställa den registrerades grundläggande fri- och rättigheter. Liksom andra begränsningar av sådana fri- och rättigheter, krävs att denna även uppfyller de andra villkor som ställs upp i artikel 52.1 i EU-stadgan (se även ovan avsnitt om uppgift av allmänt intresse). En påminnelse om att detta är av särskild vikt vid behandling av känsliga personuppgifter görs i anslutning till dessa undantag i artikel 9 i dataskyddsförordningen.

I 3 kap. dataskyddslagen finns allmänna bestämmelser om när det är tillåtet att behandla känsliga personuppgifter med stöd av undantagen i artikel 9.2 b, g och h GDPR. I 3 kap. 3 § dataskyddslagen anges att sådana uppgifter får behandlas av myndigheter med hänsyn till ett viktigt allmänt intresse om (1) uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, (2) behandlingen är nödvändig för handläggningen av ett ärende, eller (3) i annat fall, om behandlingen är nödvändig

med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Vid tillämpningen av denna bestämmelse ska andra än myndigheter i vissa fall jämställas med myndigheter. Bestämmelsen kan dock inte i sig användas för vissa sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Sådana utsökningar måste alltså ha stöd i någon annan författning. När det är tillåtet att behandla känsliga personuppgifter på området för social trygghet och socialt skydd respektive i hälso- och sjukvård och social omsorg framgår av 3 kap. 2 och 5 §§ dataskyddslagen.

Utlämnande

Datadelning innebär att en individ eller organisation gör sina data tillgänglig för andra. Eftersom ”utlämnande” av personuppgifter räknas som ”behandling” i dataskyddsrättslig mening, måste utlämnandet ha en rättslig grund och leva upp till de andra krav som föreskrivs i EU:s dataskyddsförordning och kompletterande svensk nationell lagstiftning. I det här avsnittet diskuteras dels när något ska räknas som ett ”utlämnande” av personuppgifter, dels vad som krävs för att en myndighet ska uppfylla kraven på rättslig grund, ändamålsbegränsning och öppenhet i samband med att den lämnar ut sådana uppgifter.

Utlämnande av personuppgifter

Begreppet ”utlämnade” av personuppgifter förekommer på ett antal ställen i EU:s dataskyddsförordning, men definieras inte i förordningen. Det framgår dock av den uppräkning av behandlingsåtgärder som görs i artikel 4.2 GDPR att ett utlämnande i sig utgör en ”behandling” av personuppgifter i dataskyddsrättslig mening. Det innebär att varje utlämnade måste ha en rättslig grund och leva upp till de andra krav som ställs upp i förordningen. Utlämnande utgör alltså inte endast ett osjälvständigt led i någon annan personuppgiftsansvarigs insamling. Utlämnande respektive mottagande ska snarare förstås som självständiga behandlingsåtgärder, som var för sig måste vara förenliga med de grundläggande principer för behandling av personuppgifter som anges i artikel 5 GDPR (EUD mål C-175/20 Valsts ieņēmumu dienests, punkt 61).

Med ”utlämnande” avses åtgärder där personuppgifter görs tillgängliga för någon annan genom ”överföring, spridning eller tillhandahållande på annat sätt” (artikel 4.2 GDPR). Det första rekvisitet är uppfyllt när uppgifterna har gjorts tillgängliga för någon som är ”tredje part” (artikel 4.10 GDPR), men det är inte klart om ett utlämnande ska anses ha ägt rum redan genom att uppgifterna har gjorts tillgängliga för andra ”mottagare” (artikel 4.9 GDPR) enligt dataskyddsförordningen. Eftersom ett utlämnande måste ha ägt rum för att någon ska räknas som ”mottagare” enligt definitionen i förordningen, vore det ur rättssystematisk synpunkt dock olämpligt att utsträcka begreppet till personer som inte omfattas av artikel 4.9 GDPR (Arning & Rothkegel 2022 s. 126). Om denna definition även omfattar anställda och andra som behandlar personuppgifter under den personuppgiftsansvariges överinseende, har tidigare inte ansetts vara klart (se dock mål C-579/21 Pankki S, punkt 73, som inte anser att dessa utgör mottagare).

Med ”överföring” avses att uppgifterna har lämnats ut till en eller flera bestämda mottagare medan ”spridning” innebär att uppgifterna har gjorts tillgängliga för en obestämd krets av personer (Arning & Rothkegel 2022 s. 127–128). Med hänsyn till att det räcker att ett av dessa villkor är uppfyllda uppkommer dock normalt inga gränsdragningsproblem. I många situationer är det inte särskilt viktigt om delningen av data förstås som en ”överföring” eller som ”spridning”. Vad som utgör en ”överföring” har främst betydelse för att avgöra om de särskilda bestämmelserna i kapitel V i dataskyddsförordningen om överföring till tredjeland är tillämpliga vid ett utlämnande (se EUD mål C-101/01 Lindqvist, punkt 71, om att det inte utgör en överföring till tredjeland när personuppgifter läggs ut på en webbsida som är lagrad i en medlemsstat även om uppgifterna blir åtkomliga för personer i tredjeland). När det gäller andra utlämnanden är det tillräckligt att uppgifterna har tillhandahållits på något annat sätt (artikel 4.2 GDPR). Det framgår av definitionen av begreppen att ”överföring” och ”spridning” endast är olika sätt på vilka personuppgifter kan tillhandahållas. Det avgörande är alltså om den personuppgiftsansvarige, oberoende av metod, har tillhandahållit uppgifterna. Det räcker alltså att dessa blivit tillgängliga för någon annan (till exempel genom att någon utomstående fått åtkomst till myndighetens datorsystem). När uppgifterna blivit tillgängliga genom dataintrång eller annan obehörig åtkomst (artikel 4.12 GDPR) rör det sig dock inte om ett utlämnande (Schild 2022 s. 280).

Rättslig grund

För att personuppgifter ska få lämnas ut av en myndighet krävs att utlämnandet har en rättslig grund enligt artikel 6 GDPR (se även föregående avsnitt om insamling för en utförlig diskussion om rättslig grund). En myndighet måste, som tidigare konstaterats, normalt grunda ett utlämnande på rättslig förpliktelse (artikel 6.1 c) eller uppgift av allmänt intresse (artikel 6.1 e). Vilka rättsliga ramar som gäller för ett utlämnande, beror dock på vem som är mottagare, om utlämnandet grundas på en begäran samt om det är myndigheten som på eget initiativ har gjort uppgifterna tillgängliga.

När ett privaträttsligt subjekt, såsom ett bolag, en förening eller en privatperson, har begärt att få ta del av uppgifter som förvaras hos en myndighet, kan den senare ha skyldighet att göra uppgifterna tillgängliga enligt bestämmelserna om allmänna handlingars offentlighet (2 kap. tryckfrihetsförordningen). Enligt svensk nationell rätt ska EU:s dataskyddsförordning inte tillämpas om det strider mot dessa bestämmelser i tryckfrihetsförordningen (1 kap. 7 § dataskyddslagen). En sekretessprövning ska i stället göras enligt offentlighets- och sekretesslagen (OSL), varvid myndigheten bland annat ska pröva om personuppgifterna efter utlämnandet kan antas komma att behandlas i strid med dataskyddsförordningen, dataskyddslagen eller 6 § etikprövningslagen. Artiklarna 85 och 86 GDPR ger medlemsstaterna ett utrymme att införa bestämmelser i sin nationella rätt för att sammanjämka rätten till skydd av personuppgifter med yttrande- och informationsfriheten samt allmänhetens tillgång till allmänna handlingar. De svenska reglerna har dock ifrågasatts, eftersom det är oklart om de verkligen överensstämmer med unionsrätten (Guldbrandzén & Herlin-Karnell 2022).

När någon framställer en begäran om tillgängliggörande av data för vidareutnyttjande kan tillgängliggörandet även omfattas av lagen (2022:818) om den offentliga sektorns tillgängliggörande av data (öppna datalagen). Detsamma gäller när en myndighet på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas, eller när data lämnas till en statlig eller kommunal myndighet som ska använda dem i en konkurrensutsatt verksamhet som avser tillhandahållande av data (8 § första stycket 2 och 3 öppna datalagen). Lagen ska dock inte tillämpas i andra fall när data lämnas mellan myndigheter (8 § andra stycket). Lagen som införlivar direktiv (EU) 2019/1024 i svensk nationell rätt påverkar dock inte tillämpningen av bestämmelserna i unionsrätten och nationell rätt om skydd av personuppgifter (artikel 1.4 i direktivet). För vidareutnyttjande av data som förvaras av myndigheter och skyddas av dataskyddsförordningen, men faller utanför direktivets tillämpningsområde, gäller i stället förordning (EU) 2022/868 (dataförvaltningsakten), som blir tillämplig den 24 september 2023. Förordningen påverkar dock inte tillämpningen av unionens dataskyddsregler (artikel 1.3 i förordningen) och tillgång till personuppgifter får endast beviljas om dessa har anonymiserats eller när det sker i överensstämmelse med dessa regler (artikel 5 i förordningen; Holtz & Ledendal 2023, s. 380-384).

En grundlagsfäst rättighet att ta del av allmänna handlingar har inte andra myndigheter, men myndigheter har en på förvaltningslagen (FL) grundad skyldighet att samverka med varandra (8 § FL). 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 också 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, 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 ut uppgifter till en annan myndighet finns i 6 kap. 5 § OSL. 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.

Ändamålsbegränsning

Som redan har diskuterats ovan, får personuppgifter endast samlas in för särskilda ändamål som ska bestämmas i samband med insamlingen. För att en myndighet ska få lämna ut personuppgifter till en annan myndighet, måste myndigheten enligt principen om ändamålsbegränsning (artikel 5.1 b GDPR) normalt pröva om uppgifterna efter utlämnandet kommer att behandlas på ett sätt som är förenligt med de ändamål för vilka dessa ursprungligen samlades in. Om den senare behandlingen är oförenlig med det ursprungliga ändamålet, är det endast tillåtet att lämna ut data om utlämnandet grundas på den registrerades samtycke, på unionsrätten eller på en medlemsstats nationella rätt (artikel 6.4 GDPR).

Ändamålsförändrande behandling och förenlighetsbedömning

Principen om ändamålsbegränsning (i snäv bemärkelse) gör skillnad mellan (1) insamling av personuppgifter och (2) senare behandling av dessa. Med insamling avses alla åtgärder som den personuppgiftsansvarige vidtar för att erhålla personuppgifter, oavsett om dessa samlats in direkt från den registrerade eller erhålls på något annat sätt. I mål C-77/21 Digi, har EU-domstolen slagit fast att uttrycket ”senare” ska innefatta all behandling av personuppgifter som sker efter den ursprungliga behandlingen, oberoende av ändamålet med den senare behandlingen (punkt 31). Detta synsätt överensstämmer med Artikel 29-gruppens tolkning (yttrande 3/2014, s. 21). Artikel 5.1 b, gör alltså skillnad mellan den allra första behandlingsåtgärden (insamlingen) och alla därpå följande behandlingsåtgärder. Med ledning av denna tolkning slog domstolen i ovanstående mål fast att det utgjorde en senare behandling när den personuppgiftsansvarige ”i en nyskapad databas, registrerar och lagrar personuppgifter som redan förekommer i en annan databas” (punkt 29).

Om en senare åtgärd har ett annat ändamål än det ändamål som preciserades när data samlades in, är det nödvändigt att göra en förenlighetsbedömning. En förenlighetsbedömning ska, enligt domstolen, endast göras när ”ändamålen med den senare behandlingen inte är identiska med ändamålen med den ursprungliga insamlingen” (mål C-77/21 Digi, punkt 34). EU-domstolen har i ett senare mål gjort bedömningen att det rör sig om ett nytt ändamål när personuppgifter i en personalliggare som upprättats för skattekontroll (det ursprungliga ändamålet) senare behandlas i samband med handläggning av mål i en domstol (mål C-268/21 Norra Stockholm Bygg, punkt 36).

När det rör sig om ändamålsförändrande behandling (vidarebehandling) ska en bedömning göras av om det nya ändamålet är förenligt med de ursprungliga ändamålen. En sådan förenlighetsbedömning ska göras enligt de kriterier som anges i artikel 6.4 led a till e GDPR.

- **Koppling mellan ändamålen**: Den koppling som finns mellan de ändamål för vilka personuppgifterna ursprungligen samlades in och ändamålet med vidarebehandlingen.

- **Sammanhanget**: Det sammanhang i vilket personuppgifterna ursprungligen samlades in, särskilt förhållandet mellan den personuppgiftsansvarige och den registrerade.

- **Personuppgifternas art:** Särskilt om det rör sig om känsliga personuppgifter (artikel 9 GDPR) eller personuppgifter som avser lagöverträdelser som innefattar brott (artikel 10 GDPR), som till sin natur kan innebära betydande risker för den registrerade.

- **Konsekvenser för den registrerade**: Negativa konsekvenser som kan uppkomma för den registrerade till följd av vidarebehandlingen, särskilt ingrepp i dennes rätt till privatliv eller andra grundläggande fri- och rättigheter.

- **Skyddsåtgärder**: Förekomsten av lämpliga skyddsåtgärder som vidtagits för att minska riskerna för den registrerade både beträffande den ursprungliga behandlingen och vidarebehandlingen.

Den uppräkning som görs i artikel 6.4 är som framgår av bestämmelsens ordalydelse (”bland annat”) inte uttömmande. Det är dock inte helt klart vilka andra kriterier som ska beaktas. EU-domstolen har dock konstaterat att dessa kriterier visar att det måste föreligga ett ”konkret, logiskt och tillräckligt nära samband” mellan de ursprungliga och de nya ändamålen. Domstolen menar också att kriterierna förhindrar att vidarebehandlingen avviker från de registrerades berättigade förväntningar om hur deras personuppgifter kan komma att användas (mål C-77/21 Digi, punkt 36). Vidare har domstolen förklarat att kriterierna:

> *gör det möjligt att reglera återanvändningen av tidigare insamlade personuppgifter genom att säkerställa en balans mellan, å ena sidan, behovet av förutsägbarhet och rättssäkerhet vad gäller de ändamål dessa uppgifter ursprungligen samlats in för och, å andra sidan, medgivandet av en viss flexibilitet till förmån för den personuppgiftsansvarige vid hanteringen av uppgifterna, vilket bidrar till att uppnå målet att säkra en enhetlig och hög skyddsnivå för fysiska personer. (punkt 37).*

Undantag vid uppgiftsskyldighet mellan myndigheter

När personuppgifter lämnas ut för vidarebehandling ska den personuppgiftsansvarige normalt göra en förenlighetsbedömning. Högsta förvaltningsdomstolen har dock ansett att när en myndighet lämnar ut personuppgifter till en annan myndighet enligt 6 kap. 5 § OSL, ska det inte göras någon prövning av om behandlingen är förenlig med principen om ändamålsbegränsning i artikel 5.1 b i GDPR (HFD 2021 ref. 10). Genom den föreskrivna uppgiftsskyldigheten, och de sekretessbestämmelser som hindrar myndigheter från att lämna ut integritetskänsliga uppgifter till andra myndigheter, får lagstiftaren redan anses ha tagit ställning till när ett sådant utlämnande är oförenligt med de ändamål för vilka uppgifterna ursprungligen samlades in. Utöver en sekretessprövning ska en myndighet inte göra någon kontroll av utlämnandets förenlighet med principen om ändamålsbegränsning. Ett utlämnande enligt 6 kap. 5 § OSL, måste dock fortfarande överensstämma med de andra krav som ställs upp i artikel 5 i GDPR. Exempelvis får inte fler personuppgifter lämnas ut än vad som är motiverat av ändamålet med den vidare behandlingen (artikeln 5.1 c).

Vad som inte uttryckligen behandlas i domen är i vilken utsträckning den mottagande myndigheten behöver göra en sådan prövning. Däremot konstaterade HFD att de i målet aktuella specialbestämmelserna endast gällde för den utlämnande myndigheten och alltså inte var tillämpliga på den vidare behandling som den mottagande myndigheten hade för avsikt att utföra. En sådan behandling skulle i stället prövas mot de särskilda bestämmelser som gällde för denna verksamhet. Det är med domstolens synsätt alltså den myndighet som har begärt att få ta del av personuppgifter enligt 6 kap. 5 § OSL, som ensam har att pröva om den insamling och vidare behandling som de vill göra överensstämmer med principen om ändamålsbegränsning med hänsyn taget till de eventuella registerförfattningar eller liknande specialbestämmelser som kan finnas i svensk nationell rätt.

Undantag från förbudet mot oförenlig vidarebehandling

Artikel 5.1 b GDPR innehåller ett allmänt förbud mot oförenlig vidarebehandling av personuppgifter. Detta förbud mjukas dock upp av två undantag. Om ett utlämnande eller annan senare behandling är oförenlig med de ändamål för vilka uppgifter ursprungligen samlades in, är vidarebehandlingen ändå tillåten om den grundas på den registrerades samtycke, på unionsrätten eller på en medlemsstats nationella rätt (artikel 6.4 GDPR). Som har diskuterats ovan, är möjligheterna för en myndighet att grunda behandlingen på samtycke från den registrerade begränsade (artikel 6.1 a GDPR). Det som många gånger återstår är alltså att grunda vidarebehandlingen på uppgift av allmänt intresse eller myndighetsutövning som ankommer på den personuppgiftsansvarige (artikel 6.1 e GDPR). En sådan uppgift ska ha fastställts i unionsrätten eller i en medlemsstats nationella rätt.

Det räcker enligt EU-domstolen dock inte att vidarebehandlingen har stöd i nationell rätt. Enligt artikel 6.4 GDPR måste vidarebehandlingen också utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle och skydda ett av de mål som avses i artikel 23.1 GDPR (EUD mål C-268/21 Norra Stockholm Bygg, punkt 37). För att skydda dessa viktiga mål av allmänt intresse, har den personuppgiftsansvarige rätt att vidarebehandla personuppgifter oberoende av om den senare behandlingen är förenlig med de ändamål för vilka personuppgifterna ursprungligen samlades in eller inte (skäl 50 GDPR). En sådan bestämmelse utgör alltså ett lagstadgat undantag från det allmänna förbudet mot oförenlig vidarebehandling (artikel 5.1 b GDPR). För att en bestämmelse i nationell rätt ska kunna användas som grund för vidarebehandling, måste det göras en prövning av om de förutsättningar som anges i artikel 6.4 GDPR är uppfyllda.

Enligt EU-domstolen saknar det betydelse om det rättsliga stödet utgör en materiell eller processuell bestämmelse i nationell rätt (EUD mål C-268/21 punkt 40). I målet, som gällde editionsplikt (i 38 kap. Rättegångsbalken), slog EU-domstolen fast att det var nödvändigt att ta hänsyn till de registrerades intressen (något som inte uttryckligen krävdes enligt de svenska bestämmelserna om edition) för att den nationella domstolen skulle kunna kontrollera om de förutsättningar som anges i artikel 6.4 GDPR är uppfyllda (punkt 46). Även om rätten till ett effektivt domstolsskydd (artikel 47 EU-stadgan), kan utgöra ett sådant viktigt allmänt intresse som anges i artikel 23 GDPR, måste den nationella domstolen även beakta berörda motstående intressen för att avgöra om den vidare behandlingen (utlämnandet av personuppgifterna som bevismedel) är tillåten (punkt 54). Den nationella domstolen är bland annat skyldig att fastställa om utlämnandet är förenligt med principen om uppgiftsminimering (artikel 5.1 c GDPR). Den kan också vara tvungen att besluta om skyddsåtgärder, till exempel begränsa allmänhetens möjlighet att ta del av handlingarna i målet (punkt 56).

Öppenhet

Behandling av personuppgifter ska som utgångspunkt vara öppen för den registrerade. Det innebär att det i princip inte är tillåtet att i hemlighet samla in personuppgifter för att till exempel bygga upp ett register utan de registrerades kännedom. Detsamma gäller alla andra åtgärder, såsom utlämnande eller samkörning av uppgifterna. Det framgår av artiklarna 13 och 14 i GDPR att den registrerade har rätt att få information om vem som har fått tillgång till de personuppgifter denne har lämnat. Mottagarna, eller åtminstone kategorier av mottagare, ska anges både 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 mål C-201/14 Bara m.fl. 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.

Insamling får endast ske för uttryckligt angivna ändamål. Dessa ska den registrerade få information om enligt artikel 13.1 c eller 14.1 c GDPR. Ändamålet får inte vara alltför allmänt hållet, utan måste beskrivas på ett sådant sätt att den registrerade får en tydlig bild av syftet med behandlingen. Den registrerade ska också informeras om de personuppgifter som denne har delat, kommer att behandlas för ett annat syfte än vad som angavs när uppgifterna samlades in (artiklarna 13.3 och 14.4 GDPR). Detta gäller oberoende av om behandlingen 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.

Anonymisering

EU:s dataskyddsförordning är i princip tillämplig vid all behandling av personuppgifter, det vill säga data som rör en identifierad eller identifierbar fysisk person. Det första en myndighet måste göra när den vill utbyta data är därför att bedöma om den datamängd man vill dela med någon annan innehåller personuppgifter eller inte. Vi har i Datalabbet undersökt möjligheten att minska riskerna för enskilda individer genom att endast dela anonym information. Det finns dock tekniska utmaningar med alla metoder för anonymisering. En avvägning måste därför 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.

Anonymisering av personuppgifter

Vad som avses med ”anonym information” eller ”anonymisering” definieras inte i EU:s dataskyddsförordning. En legaldefinition av ”anonymisering” förekommer dock i direktiv (EU) 2019/1024 om öppna data och vidareutnyttjande av information från den offentliga sektorn (öppna data-direktivet). I artikel 2.7 i direktivet anges att med ”anonymisering” avses ett ”förfarande för att göra handlingar till anonyma handlingar, som inte avser en identifierad eller identifierbar fysisk person, eller förfarandet för att anonymisera personuppgifter på ett sådant sätt att den registrerade inte eller inte längre är identifierbar”. Detta är en definition som överensstämmer med de uttalanden som görs i ingressen till EU:s dataskyddsförordning. Vilka anonymiseringsteknologier som ska anses säkerställa att den registrerade inte, eller inte längre, är identifierbar är alltså avgörande för om vissa datamängder kan utbytas mellan kommunala myndigheter eller lämnas ut till någon annan så att dessa kan vidareutnyttjas.

Artikel 29-gruppen har gjort en genomgång och analys av befintliga avidentifieringsmetoders effektivitet och begränsningar. Analysen är gjord i relation till det numera upphävda direktiv 95/46/EG, men kan i allt väsentligt sägas vara relevant också för nuvarande dataskyddsförordning. I yttrande 5/2014 lämnar arbetsgruppen rekommendationer om hur de befintliga avidentifieringsmetoderna bör hanteras. Rekommendationerna bygger på vilka kvarvarande risker för identifiering som är förknippad med respektive metod. I yttrandet beskrivs bland annat metoder som randomisering och generalisering, särskilt tillägg av brus, permutation, differentiell integritet, aggregering, k-anonymitet, l-diversitet och t-närhet. Europeiska dataskyddsstyrelsen håller nu på att ta fram en motsvarande utredning som ska ligga till grund för nya riktlinjer om anonymisering.

I sammanhanget är det också värt att nämna att anonymisering, det vill säga de åtgärder som vidtas för att avidentifiera personuppgifter, i sig utgör behandling av personuppgifter och omfattas därmed av EU:s dataskyddsbestämmelser (Artikel 29-gruppen). Avidentifieringen som sådan ska alltså, liksom annan behandling, uppfylla alla de krav som ställs upp i förordningen. Det är alltså först efter att uppgifterna inte längre kan kopplas till någon enskild individ som dessa faller utanför förordningens tillämpningsområde. För att ett utlämnade inte ska omfattas av förordningen, måste anonymisering alltså ske innan uppgifterna överförs till någon annan personuppgiftsansvarig. När

den vidare behandlingen ska äga rum inom myndigheten, krävs att denna utplånar samtliga kopior av uppgifterna, vilket innefattar samtliga säkerhetskopior.

I ingressen till dataskyddsförordningen görs vissa uttalanden om personuppgiftsbegreppet, som har relevans för bedömningen av när en avidentifieringsmetod är tillräckligt effektiv för att vidare behandling inte ska omfattas av förordningen. Bedömningen av om en enskild individ ska anses vara identifierbar eller inte, ska göras med utgångspunkt från alla hjälpmedel som rimligen kan komma att användas för att direkt eller indirekt identifiera denne. Vid bedömningen av om en sådan ”rimlig sannolikhet” föreligger, ska hänsyn tas till samtliga objektiva faktorer, såsom kostnader och tidsåtgång. Förutom befintlig teknik, såsom metoder för återidentifiering, ska hänsyn även tas till den tekniska utvecklingen. En anonymiseringsmetod behöver alltså inte ge ett absolut skydd mot identifiering, utan det är tillräckligt att det inte längre finns en rimlig sannolikhet för att en enskild individ ska kunna identifieras.

Bedömningen görs i första hand utifrån vilka hjälpmedel som den personuppgiftsansvarige själv förfogar över. Det kan till exempel handla om att den personuppgiftsansvarige förfogar över andra uppgifter som gör det möjligt att identifiera den registrerade. Samtidigt är det värt att påpeka att EU-domstolen har slagit fast att det även finns en risk för indirekt identifiering när de kompletterande uppgifterna innehas av tredje part. I mål C-582/14 Breyer, ansåg domstolen inte att det var ett hinder att den personuppgiftsansvarige behövde utnyttja de lagliga möjligheter som fanns att få ut kompletterande uppgifter från den registrerades internetleverantör för att kunna identifiera vem som hade använt en dynamisk IP-adress även när den förra behövde vända sig till en domstol eller annan behörig myndighet. Domstolen verkar alltså ha lagt ribban ganska högt och det är svårt att hävda att de uppgifter man hanterar är anonyma. Enligt domstolen är en uppgift anonym först när ”identifiering av den aktuella personen var förbjuden i lag eller omöjlig att genomföra i praktiken, exempelvis på grund av att den skulle kräva orimliga resurser i form av tid, kostnader och arbetskraft, med den följden att risken för identifiering i praktiken var försumbar” (se även mål T-550/20 SRB för ett liknande resonemang).

Pseudonymisering och kryptering av personuppgifter

Pseudonymisering och kryptering av personuppgifter gör normalt inte att uppgifterna kan betraktas som anonym information. Dessa åtgärder utgör i stället särskilda skyddsåtgärder som en personuppgiftsansvarig måste eller kan vidta för att behandlingen ska vara tillåten enligt EU:s dataskyddsförordning. Exempelvis är pseudonymisering en åtgärd som den personuppgiftsansvarige kan behöva vidta för att det ska vara tillåtet att behandla personuppgifter för arkivändamål av allmänt intresse eller forskningsändamål. Pseudonymisering är en sorts bearbetning av personuppgifter som gör att dessa enbart kan hänföras till en viss person om den personuppgiftsansvarige får tillgång till kompletterande uppgifter (artikel 4.5). I en pseudonymisering ersätts den registrerades namn eller personnummer med en nyckel som förvaras separat från övriga uppgifter i datamängden. Nyckeln ska dessutom omfattas av lämpliga tekniska och organisatoriska åtgärder som bland annat begränsar åtkomsten till dessa uppgifter. Även kryptering utgör en sådan skyddsåtgärd, som bland annat måste vidtas för att behandlingen av personuppgifter ska uppfylla kravet på tillräcklig säkerhet.

Federerad maskininlärning

En annan teknik som kan användas för att minska riskerna för den registrerade när personuppgifter ska samköras, är federerad maskininlärning (”federated learning”). Federerad inlärning är en metod för maskininlärning som bygger på att en algoritm tränas på data som är distribuerad över flera klienter (mobila enheter eller servrar) med lokalt lagrade data utan att dessa data överförs mellan klienterna. En AI-modell kan på så sätt tränas på en mycket stor datamängd, utan att till exempel personuppgifter eller annan känslig information behöver delas. Exempelvis kan personuppgifter behandlas lokalt på en användares mobiltelefon eller persondator, utan att dessa uppgifter som sådana behöver delas med leverantören av de digitala tjänster som finns på mobilen eller datorn. Tekniken skulle också kunna användas av kommunala myndigheter, som rättsligt är hindrade att lämna ut personuppgifter till varandra eller någon utomstående som vill vidareutnyttja uppgifterna i samband med maskininlärning.

Det finns för närvarande inga riktlinjer eller liknande från Europeiska dataskyddsstyrelsen beträffande AI, inklusive maskininlärning. Det är också oklart om dataskyddstyrelsen tänker behandla frågan om federerad inlärning i sina nya riktlinjer om anonymisering av personuppgifter. Integritetsskyddsmyndigheten har dock fått ett särskilt uppdrag av regeringen att ge stöd och vägledning kring frågor som rör dataskydd och innovation. För detta syfte har myndigheten bland annat inlett ett samarbete med AI Sweden kring regulatorisk testverksamhet. Det första pilotprojektet med fokus på datadelning mellan två vårdgivare genomfördes under 2022 (IMY 2023).

För närvarande är det oklart om federerad inlärning omfattas av EU:s dataskyddsförordning. Förutsatt att de uppgifter som används i den federerade inlärningen inte är anonymiserade, är omfattas dock åtminstone den behandling som sker lokalt av dataskyddsförordningen. Det är också värt att lägga märke till att personuppgiftsansvar enligt EU-domstolens praxis inte kräver att den ansvarige själv har tillgång till personuppgifterna (mål C-210/16 Wirtschaftsakademie Schleswig-Holstein). Det är heller inte klarlagt vilka riskerna är för så kallade ”model inversion attacks”, det vill säga att någon försöker återskapa träningsdata från AI-modellen. Det finns dock flera studier som visat att detta är möjligt (se bland annat Salem m.fl. 2019). Inom ramen för ovanstående pilotprojekt gjorde även IMY bedömningen att federerad inlärning kan innebära utlämnande av personuppgifter. Det finnas alltså fortfarande många frågor kring denna teknik, vilket gör det svårt att utan vidare använda den för att dela data mellan myndigheter. Metoden ska kanske, i likhet med pseudonymisering, snarare betraktas som en teknisk skyddsåtgärd.

Analys och slutsatser

AI, särskilt maskininlärning, utvecklas snabbt. Det skulle kunna bli ett värdefullt verktyg för att bättre förstå kommuninvånarnas komplexa behov och utveckla nya välfärdstjänster som bättre möter deras behov. Kommuner samlar redan idag in stora mängder data som skulle kunna användas för detta ändamål. Många gånger finns dock denna data spridd över olika förvaltningar och skulle behöva samlas ihop och samköras för att skapa en helhetsbild. En sådan delning och samkörning riskerar dock att öka risken för att enskilda individers personliga integritet hotas. Därför måste all sådan samordning ske med respekt för individernas grundläggande fri- och rättigheter. Dessa rättigheter är inte absoluta, men EU-stadgan och EU:s dataskyddsregler ställer krav på en hög skyddsnivå hos de myndigheter som vill samla in, dela och samköra data som innehåller personuppgifter.

När måste kommunala myndigheter följa EU:s dataskyddsförordning?

EU:s dataskyddsförordning gäller i princip för all behandling av personuppgifter. Det första en myndighet måste fastställa är om den data som den avser att samla in, dela eller på annat sätt behandla innehåller personuppgifter. Begreppet har genom EU-domstolens rättspraxis fått en mycket vidsträckt innebörd. Det medför att i stort sett all data som på ett eller annat sätt kan kopplas till bestämda individer omfattas av unionens dataskyddsregler. Domstolen har till exempel slagit fast att en uppgift ska räknas som en personuppgift om den behandlas i syfte att indirekt ta reda på något om en individ. Det är förvisso ett krav att uppgiften också kan användas för att identifiera individen i fråga, vilket innebär att anonyma uppgifter inte omfattas av regleringen. Samtidigt är det tekniskt svårt att anonymisera personuppgifter på det sätt som krävs enligt EU:s dataskyddsförordning (se nedan om anonymisering).

I vissa fall kan myndigheter få göra undantag från dataskyddsförordningen, men EU-domstolen gör en mycket restriktiv tolkning av sådana undantag. Domstolens fasta praxis visar att undantag bara görs om myndigheten behandlar personuppgifter för ändamål som rör den nationella säkerheten eller därmed jämförbara verksamhetsområden. För att omfattas måste det alltså inte röra sig om verksamhet som harmoniserats genom någon unionsrättsakt. Den svenska lagstiftaren har dessutom genom nationell rätt utvidgat förordningens tillämpningsområde till all annan verksamhet som inte uttryckligen är undantagen enligt dataskyddslagen. Även om delar av den kommunala verksamheten i strikt bemärkelse faller utanför unionsrättens tillämpningsområde så omfattas alltså i stort sett all kommunal verksamhet ändå av unionens dataskyddsregler. I de flesta fall måste kommunala myndigheter alltså följa förordningens bestämmelser när de delar personuppgifter. Därutöver ställer svensk nationell rätt ofta upp strängare krav för viss offentlig verksamhet (till exempel socialtjänsten).

Vem är ansvarig när kommunala myndigheter delar personuppgifter?

EU:s dataskyddsförordning bygger på ansvarsprincipen (ansvarsskyldighet), vilket innebär att det är den personuppgiftsansvarige som har det huvudsakliga ansvaret för att behandlingen uppfyller de krav som ställs i dataskyddsrätten. Begreppet ”personuppgiftsansvarig” har genom EU-domstolens rättspraxis fått en mycket vidsträckt innebörd. Det innebär bland annat att organisationer som tillsammans deltar i behandlingen av personuppgifter, inte sällan ska betraktas som gemensamt ansvariga. Det avgörande är inte vem som haft den formella behörigheten att fatta ett beslut, det avgörande är i stället vem eller vilka som faktiskt utövat ett bestämmande inflytande över ändamålen och medlen för behandlingen. Vid datadelning uppkommer särskilda svårigheter att fastställa vem som är ansvarig. Om uppgifterna delas för att uppnå ett gemensamt ändamål, rör det sig normalt om ett gemensamt ansvar. När en myndighet har begärt att få ta del av personuppgifter från någon annan, är utlämnaren respektive mottagaren däremot normalt sett ansvariga för den egna behandlingen av uppgifterna. De har till exempel en separat skyldighet att informera den registrerade om att dennes personuppgifter har lämnats ut respektive samlats in. När överföringen kräver teknisk samordning (till exempel direktåtkomst till databaser), är det dock inte alltid enkelt att separera utlämnande och mottagande. Det blir då särskilt viktigt att förtydliga vem som har ansvar för vilka delar av behandlingen. En oklar ansvarsfördelning kan nämligen innebära att dataskyddsreglerna överträds.

Vilka krav måste vara uppfyllda när kommunala myndigheter delar personuppgifter?

All behandling av personuppgifter måste överensstämma med de grundläggande principer för dataskydd som slås fast i EU:s dataskyddsförordning. Eftersom insamling och utlämnande av personuppgifter i sig utgör en behandling, måste de uppfylla dessa krav. Kraven är dock lite olika formulerade för olika ändamål. När personuppgifter behandlas som ett led i handläggningen av ett förvaltningsärende, uppkommer normalt större risker för den enskildes grundläggande fri- och rättigheter. Det finns därför anledning att göra en mer restriktiv tolkning av de grundläggande principerna för dataskydd. När uppgifterna däremot ska användas för forskning och utveckling (så kallad explorativ användning), är avsikten normalt inte att kartlägga enskilda individers personliga förhållanden. I stället ligger fokus på att till exempel förstå beteenden eller behov på gruppnivå. I det första fallet är det ofta nödvändigt att kunna identifiera vem uppgifterna avser. I det andra fallet, är man ute efter att dra upp de större mönstren och inte så intresserad av att identifiera enskilda individer.

Ändamålsbestämning

Det första den personuppgiftsansvarige måste göra innan personuppgifterna samlas in, är att bestämma ändamålet med behandlingen. Om uppgifterna ska användas för att handlägga en viss sorts ärende (till exempel fastställa om den sökande är berättigad till försörjningsstöd), är det oftast möjligt att beskriva ändamålet med behandlingen på ett preciserat sätt. Ändamålet beskrivs ofta också av den lag eller annan författning som styr verksamheten (till exempel förvaltningslagen eller socialtjänstlagen). Ett problem som uppkommer är att de ändamål som slås fast i lag inte sällan är förhållandevis allmänt formulerade. EU-domstolen verkar dock öppen för att det mer specifika ändamålet i stället formuleras genom ett beslut eller liknande. Om uppgifterna som samlas in ska användas för att utforska något, kan det dock vara svårt att närmare precisera hur uppgifterna kommer att användas. Det verkar dock som unionslagstiftaren är öppen för att ändamålet är mindre preciserat när personuppgifter samlas in för vetenskapliga forskningsändamål. Det är möjligt att detta även gäller vid andra liknande situationer.

Rättslig grund

För att en myndighet ska få samla in och behandla personuppgifter måste behandlingen ha en rättslig grund. När det gäller myndigheter följer detta delvis redan av legalitetsprincipen, men i dataskyddshänseende innebär kravet på laglighet att behandlingen måste grunda sig på någon av de sex rättsgrunder som räknas upp i dataskyddsförordningen. För myndigheter finns en begränsad möjlighet att använda samtycke eller den s.k. intresseavvägningsregeln, vilket innebär att behandlingen normalt måste grunda sig på en rättslig förpliktelse eller en uppgift av allmänt intresse som har fastställts i lag eller annan författning. Detta innebär dels som konstaterats ovan att det normalt finns ett oupplösligt samband mellan kravet på ändamålsbestämning och rättslig grund, dels att insamlingen eller utlämnandet ska ha ett författningsstöd. Det senare är en följd av att redan en myndighets insamling och lagring av personuppgifter, oavsett om dessa är känsliga, enligt rättspraxis utgör ett intrång i den enskildes rätt till privatliv. En myndighets behandling måste därför enligt EU-stadgan alltid vara föreskriven i lag.

När personuppgifterna ska användas som ett led i myndighetsutövning mot enskild, finns det begränsat utrymme för att avvika från kravet på att behandlingen ska vara föreskriven i lag. Det räcker dock inte med att en förpliktelse eller en uppgift av allmänt intresse har slagits fast i lag eller annan författning. Myndighetens användning begränsas också till vissa bestämda ändamål som kan motivera det ingrepp som användningen av personuppgifterna innebär för den registrerade. För att en nationell bestämmelse ska få användas som rättsgrund, ställs alltså vissa krav på dess precision och förutsägbarhet. Om en nationell bestämmelse inte uppfyller dessa villkor ska en myndighet, i princip avstå från att tillämpa denna bestämmelse. Möjligheten att behandla personuppgifter inom kommunal förvaltning kan alltså skifta beroende på hur den nationella lagstiftning som reglerar ett verksamhetsområde (till exempel socialtjänst, skola eller bibliotek) har utformats. Exempelvis kan bibliotekslagens utformning leda till svårigheter att behandla personuppgifter, eftersom den inte innehåller en ur dataskyddsrättssynpunkt tillräckligt precis beskrivning av på vilket sätt personuppgifterna kan komma att behandlas.

Ändamålsbegränsning

Utlämnande och vidarebehandling av personuppgifter måste dessutom överensstämma med principen om ändamålsbegränsning. Personuppgifter får nämligen endast behandlas för andra ändamål om dessa är förenliga med de ändamål för vilka de ursprungligen samlades in. Det vanliga är att varje kommunal förvaltning samlar in data genom sin ärendehandläggning eller övriga verksamhet. Ändamålet med behandlingen har då, som konstaterats ovan, normalt bestämts i lag eller annan författning. Det gör det svårare att sedan använda de insamlade uppgifterna för andra ändamål. Begränsningar i hur personuppgifterna får vidarebehandlas kan även följa av speciallagstiftning (till exempel lagen om behandling av personuppgifter inom socialtjänsten). För att det ska vara tillåtet att utlämna personuppgifter från en myndighet till en annan, måste det finnas en rättslig grund men också göras en förenlighetsbedömning. Om bedömningen visar att det nya ändamålet inte är förenligt med det ursprungliga ändamålet, är behandlingen som utgångspunkt förbjuden. Undantag görs om den vidare behandlingen är tillåten i lag eller annan författning. När så inte är fallet måste myndigheten på nytt samla in personuppgifterna från den registrerade. Anledningen till detta förfarande, är att det ger den registrerade större insyn och kontroll över behandlingen. Det är värt att lägga märke till att HFD gjort bedömningen att principen om ändamålsbegränsning inte gäller vid utlämnande mellan myndigheter enligt 6 kap. 5 § OSL.

När är det möjligt att anonymisera eller vidta andra tekniska skyddsåtgärder vid delning av personuppgifter?

När syftet med behandlingen inte kräver att den registrerade identifieras, bör myndigheten både av praktiska och rättsliga skäl överväga om målet med behandlingen kan uppnås genom att dela anonyma uppgifter. Myndigheten bör också bedöma om det finns någon lämplig metod för att göra denna anonymisering av data. Här räcker det inte att göra en pseudonymisering eller kryptering av personuppgifter, eftersom detta inte gör uppgifterna anonyma i dataskyddsrättslig mening. Även i de fall då GDPR kräver att personuppgifter ska pseudonymiseras eller krypteras, omfattas behandlingen fortfarande av GDPR:s övriga 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. EU-domstolen har slagit fast att personuppgifter ska räknas som anonyma först om risken för identifiering i praktiken är försumbar. Sådan anonymisering kan vara tekniskt svår att genomföra. Artikel 29-gruppen har lämnat vissa rekommendationer om olika avidentifieringsmetoder, men tar inte specifikt upp frågor som rör AI, inklusive maskininlärning. Nya 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 å ena sidan och möjligheten att bevara uppgifternas användbarhet och kvalitet å den andra. Det finns en risk att en gallring som sker när data ska anonymiseras leder till ett sämre resultat. En alternativ teknik kan var att använda federerad maskinlärning. Detta minskar riskerna för den

registrerade vid samkörning av personuppgifter. Eftersom denna metod bygger på att en algoritm tränas med hjälp av flera olika klienter med lokalt lagrade data utan att dessa delas mellan klienterna, kan en AI-modell 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. Det kan också vara möjligt att använda syntetiska data, det vill säga data som genereras syntetiskt i stället för att samlas in eller mätas upp. Det finns dock tekniska utmaningar med att generera syntetiska data som håller tillräckligt hög kvalitet. Både federerad maskininlärning och syntetisk data riskerar också att bli föremål för attacker som leder till obehörig åtkomst av personuppgifter. Det finns alltså få helt säkra metoder för att dela uppgifter mellan myndigheter. Det handlar alltså snarare om att hantera dessa på ett sådant sätt att riskerna minimeras, vilket kan göra behandlingen godtagbar ur integritetssynpunkt.

Referenser

Litteratur

Arning, M.A. & Rothkegel, T. (2022). Artikel 4 - Begriffsbestimmungen. I Taeger, J. & Gabel, D. (red.), DSGVO – BDSG – TTDSG – Kommentar. Upplaga 4. *Fachmedien Recht und Wirtschaft*, s. 87–249.

Artikel 29-arbetsgruppen för skydd av personuppgifter. *Opinion 3/2013 on purpose limitation* (WP 203), antaget den 2 april 2013.

Artikel 29-arbetsgruppen för skydd av personuppgifter. *Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen* i artikel 7 i direktiv 95/46/EG (WP 217), antaget den 9 april 2014.

Artikel 29-arbetsgruppen för skydd av personuppgifter. *Yttrande 5/2014 om avidentifieringsmetoder* (WP 216), antaget den 10 april 2014.

Europeiska dataskyddsstyrelsen. *Riktlinjer 4/2019 om artikel 25 inbyggt dataskydd och dataskydd som standard,* antagna den 20 oktober 2020.

Europeiska dataskyddsstyrelsen. *Riktlinjer 5/2020 om samtycke enligt förordning* (EU) 2016/679, antagna den 4 maj 2020.

Europeiska dataskyddsstyrelsen. *Riktlinjer 7/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR*, antagna den 7 juli 2021.

Europeiska dataskyddsstyrelsen. *Guidelines 9/2022 on personal data breach notification under GDPR*, antagna den 28 mars 2023.

Europeiska kommissionen. *Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning)*. COM (2012) 11 slutlig.

von Grafenstein, M. (2018). *The Principle of Purpose Limitation in Data Protection Laws: The risk-based approach, principles, and private standards as elements for regulating innovation.* Nomos Verlagsgesellschaft.

Guldbrandzén, W & Herlin-Karnell, E. (2022). *T*vivelaktig svensk tillämpning av EU:s dataskyddsregler. *Svensk juristtidning*, 107(8), s. 759–n.

Holtz, H. M. & Ledendal, J. (2020). Överlappningen mellan dataskydd och marknadsrätt – Dataskyddsförordningens tillämpning på marknadsföring och marknadsrättens tillämpning på kommersiell personuppgiftsbehandling. *Svensk juristtidning*, 105(2), s. 140–169.

Holtz, H. M. & Ledendal, J. (2023). Dataskyddsförordningen – det digitala årtiondets drottning. I Westman, D., Magnusson Sjöberg, C., Öman, S., Törngren, D. & Brinnen M. (red.), *Dataskyddet 50 år – historia, aktuella problem och framtid* (kommande), s. 379–396.

Integritetsskyddsmyndigheten (2023). *Federerad maskininlärning mellan två vårdgivare – Slutrapport om Integritetsskyddsmyndighetens pilotprojekt med regulatorisk testverksamhet om dataskydd.* 2023-03-15, dnr. IMY-2023-2602.

Kranenborg, H. (2021). Article 8 - Protection of Personal Data. I S. Peers, T. Hervey, J. Kenner, & A. Ward (red.), *The EU Charter of Fundamental Rights - A Commentary.* Upplaga 2. Hart Publishing, s. 231–289.

Ledendal, J. (2020). Samtycke till behandling av personuppgifter. I Karlsson Tuula, M., Person, A.H. & Lindskoug, P. (red.), *Festskrift till Rolf Dotevall.* Malmö: Juristförlaget i Lund, s. 401–423.

Lundmark, J. & Säfsten, M. (2020), *Förvaltningslagen – En kommentar*. Turenki: Norstedts juridik.

Madell, T. (2011). *Tjänster av allmänt intresse – ett svenskt perspektiv*. SIEPS 2011:8. Stockholm: Svenska institutet för europapolitiska studier.

Regeringen (2000). *Ny socialtjänstlag m.m.* Prop. 2000/01:80.

Regeringen (2016). *En modern och rättssäker förvaltning – ny förvaltningslag.* Prop. 2016/17:180.

Salem A., Zhang Y., Humbert M., Berrang P., Fritz M., Backes M. (2019). *ML-Leaks: Model and Data Independent Membership Inference Attacks and Defenses on Machine Learning Models*. Annual Network and Distributed System Security Symposium. arXiv preprint arXiv:1806.01246.

Schild, H. H. (2022). Artikel 4 - Begriffsbestimmungen. I Wolff, H. A. & Brink, S (red.), *Datenschutzrecht – DSGVO – BDSG – Grundlagen Bereichsspezifischer Datenschutz* – Kommentar. Upplaga 2. C.H. Beck, s. 265–308.

SOU (1999). *Behandling av personuppgifter inom socialtjänsten.* SOU 1999:109. Stockholm: Regeringskansliet.

Strömberg, H. & Lundell, B. (2018). *Allmän förvaltningsrätt.* Liber.

Öman, S. (2021). *Dataskyddsförordningen (GDPR) m.m. – En kommentar.* Upplaga 2. Warszawa: Norstedts juridik.

Lagstiftning

Europeiska unionen

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.

Europeiska unionens stadga om de grundläggande rättigheterna, EUT C 202, 7.6.2016, s. 389–405.

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.

Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn, EUT L 172, 26.6.2019, s. 56–83.

Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), EUT L 152, 3.6.2022, s. 1–44.

Sverige

Personuppgiftslag (1998:204)

Lag (2001:454) *om behandling av personuppgifter inom socialtjänsten*

Offentlighets- och sekretesslagen (2009:400)

Skollag (2010:800)

Bibliotekslag (2013:801)

Förvaltningslag (2017:900)

Lag (2018:218) *med kompletterande bestämmelser till EU:s dataskyddsförordning*

Lag (2022:818) *om den offentliga sektorns tillgängliggörande av data*

Rättsfall

Europeiska unionen

Dom den 20 maj 2003 i de förenade målen C-465/00, C-138/01 och C-139/01, *Österreichischer Rundfunk m.fl.*, ECLI:EU:C:2002:662.

Dom den november 2003 i mål C-101/01, *Lindqvist*, ECLI:EU:C:2002:513.

Dom den 16 december 2008 i mål C-73/07, *Satakunnan Markkinapörssi och Satamedia,* ECLI:EU:C:2008:266.

Dom den 16 december 2008 i mål C-524/06, *Huber*, ECLI:EU:C:2008:194.

Dom den 24 november 2011 i mål C-468/10, *ASNEF*, ECLI:EU:C:2011:777.

Dom den 13 maj 2014 i mål den 13 maj 2014, *Google Spain och Google*, ECLI:EU:C:2013:424.

Dom den 1 oktober 2015 i mål C-201/14, *Bara m.fl.*, ECLI:EU:C:2015:461.

Dom den 6 oktober 2015 i mål C-362/14, *Schrems*, ECLI:EU:C:2015:627.

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

Dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, ECLI:EU:C:2016:970.

Dom den 20 december 2017 i mål C-434/16, *Nowak*, ECLI:EU:C:2017:582.

Dom den 5 juni 2018 i mål C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2017:796.

Dom den 10 juli 2018 i mål C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551.

Dom den 16 januari 2019 i mål C-496/17, *Deutsche Post*, ECLI:EU:C:2019:26.

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

Dom den 9 juli 2020 i mål C-272/19, *Land Hessen,* ECLI:EU:C:2020:535.

Dom den 10 december 2020 i mål C-620/19, *J & S Service*, ECLI:EU:C:2020:649.

Dom den 22 juni 2021 i mål C-439/19, *Latvijas Republikas Saeima*, ECLI:EU:C:2020:1054.

Dom den 24 februari 2022 i mål C-175/20, *Valsts ieņēmumu dienests*, ECLI:EU:C:2021:690.

Dom den 1 augusti 2022 i mål C-184/20, *Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2021:991.

Dom den 20 oktober 2022 i mål C-77/21, *Digi*, ECLI:EU:C:2022:248.

Dom den 8 december 2022 i mål C-460/20, *Google (Déréférencement d'un contenu prétendument inexact)*, ECLI:EU:C:2022:271.

Dom den 8 december 2022 i mål C-180/21, *Inspektor v Inspektorata kam Visshia sadeben savet (Finalités du traitement de données - Enquête pénale)*, ECLI:EU:C:2022:406.

Dom den 2 mars 2023 i mål C-268/21, *Norra Stockholm Bygg*, ECLI:EU:C:2023:145.

Dom den 26 april 2023 i mål T-557/20, *SRB mot Europeiska datatillsynsmannen*, ECLI:EU:T:2023:219 (överklagat mål C-413/23 P).

Dom den 4 maj 2023 i mål C-60/22, *Bundesrepublik Deutschland*, ECLI:EU:C:2023:373.

Dom den 22 juni 2023 i mål C-579/21, *Pankki S*, ECLI:EU:C:2022:1001.

Sverige

HFD 2021 ref. 10

Kammarrättens i Stockholm dom 2022-11-07, mål nr 7678-21.

Integritetsskyddsmyndigheten beslut 2015-12-18, dnr. 2445-2014.

Integritetsskyddsmyndigheten beslut 2020-11-24, dnr. DI-2019-7782.

Integritetsskyddsmyndigheten beslut 2021-06-09, dnr. DI-2018-22697.

AVSLUTANDE DISKUSSION

Datadelningens dilemman i välfärdsutvecklingen

Sara Leckner, Jonas Ledendal
och Annika Nilsson

Skärningspunkter mellan etik och juridik: slutsatser och lärdomar

Syftet med delstudierna som presenterats i de två föregående kapitlen var dels att undersöka medborgarnas inställning till kommunens nuvarande och önskade dataanvändning och ge underlag för hur datadriven teknik kan användas på ett etiskt sätt, utifrån invånarnas perspektiv; dels att undersöka de rättsliga förutsättningarna för att dela data mellan kommunala myndigheter samt om de bestämmelser som gäller för kommunala myndigheter utgör särskilda hinder för att dela data och tillhandahålla digitala tjänster till sina invånare. Resultaten från de respektive delstudierna kan användas vägledande för såväl etiska avväganden som juridiska ställningstaganden för kommunen.

I detta gemensamma och avslutande kapitel diskuteras ett antal skärningspunkter, det vill säga gemensamma beröringspunkter och samband mellan det juridiska och det etiska perspektivet, där dessa påverkar varandra. Kapitlet avslutas med en diskussion om lärdomar kopplade till det praktiska utvecklingsarbetet och hur staden behöver agera för att ta vara på den kunskap som producerats i Datalabbet och stödja ett organisatoriskt lärande.

Skärningspunkt 1: invånarnas tillit bygger på strikta juridiska krav och transparens

Resultaten visar att invånarna har en relativt hög tillit till kommunen. Tre aspekter av denna tillit är särskilt relevanta att lyfta fram:

- Tilliten till kommunen grundar sig främst i en förväntad efterlevnad av de strikta juridiska krav kommunen (och andra offentliga institutioner) måste följa. Då regelefterlevnad är en viktig princip för kommunen kan det vara nog så viktigt att påminna sig om värdet av de strikta och komplexa regler som gäller för den kommunala verksamheten och att de i grunden gynnar kommunens relation till invånarna.

- Kommunen upplevs även ha invånarnas bästa för ögonen. Kommunens agerande ses därmed som mer etiskt, jämfört med många kommersiella företag. En sådan tillit är det viktigt för kommunen att arbeta för att behålla genom ett etiskt förhållningssätt när/om samkörning och liknande tekniker blir aktuella.

- En annan viktig orsak till att invånarna har tillit till kommunen, är upplevelsen av transparens. För att individen ska känna sig trygg med att dela sina data, krävs att individen har kännedom om vilka data som samlas in, vad de ska användas till och av vem. För att delningen ska uppfattas som transparent, krävs också att invånarna har kunskap om hur de ska sätta lämpliga ramar kring den personliga integriteten samt kontrollera sina data om de så önskar. Även om det är få som aktivt agerar på sin kunskap eller tar kontroll över sina data och sina rättigheter, måste det finnas möjlighet att göra det *om individen skulle vilja*. Förslagsvis skulle staden här kunna ut-

veckla tydligare processer för ”rätten att bli glömd” och vid vilka situationer individen kan ”klippa” sin datadelningskedja. Om staden utforskar möjligheten att samköra data som är insamlad för ett eller flera andra syften än det som är målet med samkörningen, är det särskilt viktigt att arbeta för att processen blir transparent och kontrollerbar för individen. En av anledningarna till det är att synen på, och viljan till, datadelning är högst kontextuell. Ändras förutsättningarna – det vill säga att delad data används för andra syften än för vilka de delades – kan också individens inställning till delningen ändras.

Skärningspunkt 2: anonymisering är önskvärt men svårt juridiskt och tekniskt

En aspekt som utforskats är invånarnas attityder till om anonymisering av data skulle kunna minska eller till och med eliminera den oro som finns kring datadelning. Nationella studier har visat att om den delade informationen inte går att spåra till individen, minskar oron för integritetsmissbruk vilket ökar den upplevda tryggheten. Resultaten visar dock att kommunen redan anses vara en trygg aktör att dela data med, och att anonymisering därmed inte är lika viktigt. Snarare är det många som tycker tvärt om: om data anonymiseras, hur ska kommunen då kunna hjälpa den enskilde medborgaren? Denna syn på anonymisering av data förändras dock när invånarna ställs inför nya och för dem okända sätt att hantera data inom kommunen (som den föreslagna förvaltningsgemensamma samkörningen). I mötet med nya tekniker, är det fler som tycker att anonymisering är viktigt. Resultatet tyder på att det som är mindre välkänt upplevs som mer osäkert för individen. Anonymisering är dock svårt att genomföra, både utifrån ett tekniskt perspektiv (så att data till exempel inte bara blir pseudonymiserade) och ett juridiskt perspektiv (till exempel när det gäller att bedöma var anonymiseringen ska ske, i vilken verksamhet och av vem). De tekniska svårigheterna riskerar att undergräva nyttan av metoderna och i förlängningen påverka invånarnas tillit till kommunen negativt.

Skärningspunkt 3: Kunskap om teknik och juridik viktig för tilliten, och behöver stärkas kontinuerligt

Resultatet indikerar en relativt hög kunskapsnivå hos invånarna om vad datahantering innebär. En hög kunskapsnivå är något som kan påverka inställningen till kommunens dataanvändning positivt. Att ha hög kunskap på område ska dock inte tolkas som att invånarna är odelat okritiska, även om tidigare studier visar på ett samband mellan hög kunskapsnivå och positiv inställning. Dock hänger kunskap ihop med känslan av kontroll vilket i sin tur bidrar till tilliten till kommunen.

Den höga (självskattade) kunskapsnivån hos de svarande kan vara ett resultat av att kommunen under en längre tid har arbetat aktivt med kommunikation om nyttan med digitalisering och innovation, vilket nu ger genomslag hos invånarna. Men det kan också vara en effekt av att personer med lägre utbildningsnivå (jfr. invånarnas demografiska profil med andra kommuners) inte har förmågan att se sina egna tillkortakommanden och upplever sig ha större kunskaper än de faktiskt har. Oavsett bör kommunen arbeta vidare med kunskapshöjande aktiviteter, om såväl juridiska rättigheter som tekniska möjligheter, för att bidra till transparens och stödja invånarnas förmåga att delta och påverka kommunens digitalisering på ett medvetet och tryggt sätt.

När man tittar närmare på invånarnas kunskapsnivå framkommer det att de inte besitter någon djupare teknisk kunskap. Detta kan inte heller förväntas hos gemene man. Bristen på djupare tekniska kunskaper gör dock att det är svårare för invånarna att ta ställning till frågor kring framväxande teknik och vad det kan innebära för dem. Det gjorde det också svårt vid intervjuerna att få djupgående svar från invånarna om deras inställning till kommunens önskade samkörning. Kunskapsbrist hos respondenter är inte en unik utmaning för den här studien, utan något som uppmärksammats också i annan forskning kring attityder till datadelning. Här behöver kommunen arbeta vidare med att konkretisera specifika tjänster och användningsområden relaterade till datadelning. Det är nämligen ofta lättare för invånarna att ta ställning till konkreta förslag, än abstrakta möjligheter. Kunskapshöjande åtgärder bör ses som en viktig aktivitet i stadens utvecklingsprojekt, för att säkerställa invånarnas tillit.

Sammanfattningsvis visar resultaten att invånarna i nuläget förutsätter att kommunen redan samkör data. Därmed tycks inte samkörning som sådan vara något problem, förutsatt att regelverket efterföljs. Det innebär att invånarna lägger över en stor del av kontrollen av sin integritet på kommunen, vilket ytterligare talar för att kommunen behöver involvera invånarna i sin digitalisering av tjänster och motivera dem att mer aktivt agera och ta kontroll över sin integritet. Rekommendationerna från denna delstudie är därmed att grundstenarna i kommunens digitaliseringsarbete bör vara att 1, behålla den tillit som finns och 2, motivera invånarna att mer aktivt agera och ta kontroll över sin integritet.

Slutsats

Datalabbets **primära mål** var att identifiera ett juridiskt gångbart koncept för stordataanalyser baserat på invånardata från två eller fler förvaltningar samt att undersöka invånarnas inställning till att anonymiserad data används på ett rättssäkert sätt för att bättre förstå invånarnas komplexa behov och kunna designa förvaltningsövergripande kommunala tjänster med ökat värdeskapande för invånaren. Ytterligare en målsättning med Datalabbet var att kunna presentera ett antal prototyper på offentliga tjänster som designats utifrån de insikter om invånares komplexa behov som samkörningen och attitydundersökningen resulterat i.

Labbet nådde inte den primära målsättningen att hitta ett juridiskt gångbart sätt att samköra data mellan två förvaltningar. Dock har staden fått en klarare bild av det gällande rättsläget och hur den rådande lagstiftningen ska tolkas. Kunskapen har därmed ökat, särskilt kring *varför* data ibland inte kan samköras. Därtill har de nya insikter om invånarnas attityder till kommunens hantering av data visat att det finns en diskrepans mellan invånarnas attityder och juridikens handlingsutrymme. I flera fall var invånarna mer positiva till nya sätt att hantera personliga data, än vad lagen ger handlingsutrymme till. Resultaten från delstudierna gjorde att man inte lyckades utveckla några prototyper på nya offentliga tjänster inom Datalabbet. Istället återfördes löpande lärdomar från Datalabbet in i stadens organisation och i andra utvecklingsprojekt. Den ökade förståelse för GDPR och relaterad lagstiftning medförde ett större fokus på utvecklingsprojekt där man analyserar data *inom* respektive förvaltning.

Datalabbets **sekundära mål** var att försöka påverka lagstiftaren att undanröja identifierade juridiska hinder så att nya och mer värdeskapande offentliga tjänster kan erbjudas till invånaren, om det skulle visa sig finnas en diskrepans mellan invånarnas attityder och juridikens handlingsutrymme.

En viktig slutsats från projektet är att de hinder som finns för att dela eller samköra data för att på ett bättre sätt utföra de uppgifter som åligger kommunen inte sällan beror på att den svenska lagstiftningen inte i tillräckligt hög grad anpassats till EU:s dataskyddsrätt. Det rör sig till exempel om att de nationella bestämmelser som behandlingen ska grunda sig på inte ger tillräckligt tydliga ramar. Något som också är viktigt för tilliten. Att det råder oklarheter om rättsläget kan även vara ett hinder i sig. De förändringar av lagstiftningen som kan behövas är alltså inte nödvändigtvis att likställa med en sänkning av skyddsnivån för personuppgifter, utan handlar snarare om bättre anpassningar och att använda det handlingsutrymme som medlemsstaterna har enligt GDPR.

Att förändra lagstiftningen är ingenting som görs i en handvändning, men inom projektet har påverkansarbetet drivits genom satsningen #bättredelat, genom projektet DRIV (som drivs av Lindholmen Science Park), i samarbete med AI Sweden, och i direktkontakt med Integritetsskyddsmyndigheten (IMY) och Myndigheten för digital förvaltning (DIGG). IMY har, jämte sin tillsynsverksamhet, också börjat arbeta med mer och djupare handledning, bland annat i form av innovationshubbar och regulatoriska sandlådor. Detta bidrar till att skapa en ömsesidig förståelse för arbetssätt, processer och hinder i lagstiftningen, och har visat sig vara en mer framkomlig väg för påverkansarbete än att försöka påverka lagstiftningen direkt.

Organisatoriskt lärande

Förutom en djupare förståelse för invånarnas attityder till datahantering i en kommun och juridiken som reglerar densamma, kan vi dra flera lärdomar av processen och arbetet i labbet som är viktiga att återkoppla till den kommunala organisationen. För det första behöver staden bli bättre på att kommunicera nyttan med dataanalyser. Genom Datalabbets genomförande har visionen om vad man kan uppnå genom att dela data, ställts mot invändningen att det vet man inte förrän man har provat. Man hamnar i ett moment 22: det är svårt att tänka sig förbi de juridiska hindren och föreställa sig vilka insikter man får av att samköra data, och vilka nya tjänster man skulle kunna utveckla ur dessa insikter, utan att faktiskt göra samkörningen. Samtidigt är det svårt att förankra ett utvecklingsarbete inom organisationen och att involvera invånarna utan att först förutse vilka värden som kan komma ut ur en sådan process.

I många fall förväntas medarbetare också agera i någon form av hybridfunktion och bidra med nya lösningar som vanligtvis inte ligger inom deras ordinarie arbete. Dataförvaltare ska hitta kreativa lösningar i gränssnitt med andra förvaltningars data. Praktiker inom skola och socialtjänst ska se möjligheterna med data och uppmuntras hitta innovativa digitala lösningar till problem i verksamheten. Hybridfunktionernas arbete försvåras av att det finns en föreställning om att digitalisering och data är svårt och abstrakt. Det skulle därför behövas metoder som kan visualisera potentialen med dataanalyser och datadelning. Det skulle göra det lättare att skapa samsyn kring arbetssättet och göra värdet av de tjänster man vill skapa mer konkret. Framtidsscenarios, framtidsprotyper eller spekulativ design är några sådana metoder som skulle kunna testas. Det skulle innebära att man kopplar in ännu fler funktioner och metoder i ett redan komplicerat arbete, men förhoppningsvis vinner alla involverade på en gemensam retorik och ökad tydlighet i kommunikationen.

För det andra, behöver organisationen arbeta in mer självreflektion i digitaliseringsfrågan och gällande dataanalyser. Nästan alla medarbetare i kommunen arbetar med digitalisering i någon utsträckning. Under arbetet med Datalabbet har vi märkt en ökad mognad i frågan och att allt fler ser möjligheter med att använda data för att utveckla verksamheten. Samtidigt har digitalisering och dataanalys oreflekterat börjat ses som lösningen på många av välfärdsfrågorna. Tilltron till att digitalisering ska göra arbetet i kommunen mer effektivt och möjliggöra att vi kan leva upp till ökade krav med mindre resurser är stor. Till stora delar är det här resonemanget hämtat från den privata sektorn och utgår från näringslivets förutsättningar. Vilka effekter och besparingar dataanalyser kan bidra med i den offentliga sektorn behöver kontinuerligt utvärderas. Digitaliseringens möjlighet att effektivisera välfärdsarbetet behöver konkretiseras och skärskådas utifrån den faktiska verksamheten. Bara på så sätt kan vi få en mer nyanserad och relevant bild av vad som kan uppnås.

För det tredje, behöver organisationen bli bättre på att arbeta strategiskt med det ”osäkra” och komplexa. Datalabbet har visat att det sällan finns enkla svar. I stället behöver man ofta hantera motsägelser när man arbetar med data och utveckling. Inte minst juristerna, som är vana vid att arbeta med rätt eller fel, lagligt eller olagligt, utmanas att ta ställning utifrån ett mer oklart rättsläge.

De behöver kunna resonera med och vägleda sina kollegor i dessa ställningstaganden och arbeta nära det praktiska utvecklingsarbetet. Men även digitaliseringsorganisationen behöver ställa om för att hantera såväl det operativa och förvaltande arbetet som ett strategiskt digitaliseringsarbete. Ska verksamheten utvecklas krävs en förmåga att röra sig på okänd mark samt en kapacitet att söka och ta in ny kunskap och göra kontinuerliga avvägningar. Det krävs också att man kan hantera frågor kring etik och demokrati över olika funktioner oavsett förvaltningsgränser. Detta är ett sätt att arbeta som inte tillåts av rådande organisation och arbetssätt. Att hitta dessa nya sätt att arbeta med det ”osäkra” och komplexa är en utmaning inte bara i Helsingborgs stad, utan också för hela den svenska offentliga sektorn. Det sammanhang där man verkar ha tagit sig an dessa frågor mest framgångsrikt verkar vara i IMY:s regulatoriska testverksamhet. Detta sätt att arbeta kan vara värt att titta närmare på även i Helsingborg.

Behoven av att effektivisera och innovera i den offentliga sektorn är stora och utmanande. När det kommer till innovation baserad på digitalisering, data och AI tillkommer dessutom utmaningar i gränslandet mellan teknik, juridik och etik. Det finns ett stort behov av att utveckla den kompetens som behövs för att arbeta med innovation inom ramen för de legala förutsättningar som alla länder inom EU gemensamt har att förhålla sig till. I det arbetet behövs det team bestående av professioner som kan röra sig i gränslandet mellan teknik, juridik och etik, och som tillsammans har kapacitet att identifiera och hantera sådana frågor. De måste också ha förmåga att arbeta nära förvaltningarna och förstå praktikens förutsättningar. Troligtvis kommer även de nationella myndigheterna att ställa krav på sådan tvärsektoriell och juridisk kompetens framöver, till exempel för att finansiera projekt eller för att arbeta med regulatoriska sandlådor.

Förhoppningsvis kan denna rapport vara ett bidrag i den utvecklingen och komma till användning inte minst inom kommunala tvärfunktionella digitaliserings- och innovationsteam. Genom att ge strateger, tekniker, jurister, chefer och i förlängningen också medborgare, en gemensam förståelse och ett gemensamt språk för de rättsliga och etiska frågorna kan kunskapsklyftorna utjämnas och maktfördelningen i teamen bli mer jämlik. Det är ett viktigt steg i riktningen mot att arbeta smartare tillsammans i de här frågorna.

Författarpresentation

Sara Leckner är docent i medieteknik och universitetslektor vid Institutionen för datavetenskap och medieteknik, Malmö universitet. Hennes forskning handlar om attityder och beteenden i relation till utvecklingen av digitala och datadrivna tjänster och marknader.

Jonas Ledendal är jur.dr. och universitetslektor vid Institutionen för handelsrätt, Ekonomihögskolan vid Lunds universitet. Han forskar om europeisk datarätt, särskilt frågor som rör öppna data, datadelning och dataskydd.

Annika Nilsson är forsknings- och transformationsledare på Avdelningen för innovation och transformation, Helsingborgs stad. Hon har en bakgrund inom statsvetenskap och hållbar stadsutveckling och har mångårig erfarenhet av samverkansprojekt mellan akademi och kommunal offentlig sektor.