MANOLIS NYMARK CONSULTING

PROMEMORIA

2018-10-27

Laglighetsprövning av tjänsten Embrace

Sammanfattning – slutsatser och rekommendationer

1. Embrace är en molntjänst avsedd för brottsförebyggande lokal samverkan, t.ex. mellan polis, kommun och näringslivet. Embrace gör det möjligt att bedriva sådan samverkan både på ett kunskapsbaserat och metodiskt sätt. En central funktion i Embrace är den gemensamma lokala problembilden (Embrace Insight). Det är en grafisk översiktsbeskrivning av var och när saker sker och hur utvecklingen över tid ser ut. Alla lokalt samverkande parter som använder Embrace bidrar med information till den gemensamma problembilden, och kan ta del av densamma. Embrace bygger på en metod (kunskapsbaserat arbete i samverkan) som förespråkas av Brottsförebyggande rådet (Brå), Polismyndigheten och Sveriges Kommuner och Landsting vid lokalt brottsförebyggande arbete. Embrace utvecklas av Embrace Safety AB i samverkan med bl.a. Polismyndigheten och ett flertal kommuner.

2. Embrace registrerar inte enskilda individer utan enbart brottsrelaterade och andra otrygghetsskapande händelser. Embrace är inte designat för att registrera individuppgifter, och tekniska och administrativa mekanismer finns inbyggda i tjänsten för att förhindra sådan registrering. För att kunna analysera brottsrelaterade och andra otrygghetsskapande händelser samt följa upp motverkande insatser krävs emellertid registrering av exakta platsuppgifter, t.ex. gatu- och adressuppgifter. Sådana uppgifter kan *indirekt* hänföras till en fysisk levande person som har sitt hushåll på adressen eller stadigvarande vistas där, t.ex. en familj vars villa har utsatts för skadegörelse på fasaden. Övervägande skäl talar därför för att Embrace *i dessa fall* behandlar *personuppgifter* i både dataskyddsförordningens och brottsdatalagens mening, trots att det inte är det huvudsakliga syftet med tjänsten att registrera enskilda individer. Registrering av händelser som inträffar på allmänna platser, t.ex. torg, parker eller köpcentra utgör däremot inte personuppgifter eftersom dessa adressuppgifter inte eller sällan kan hänföras till enskilda individer på något sätt.

3. Embrace är ett datoriserat register och omfattas därmed av dataskyddsförordningens, dataskyddslagens respektive brottsdatalagens och polisdatalagens bestämmelser. Vilka av dessa författningar som blir tillämplig på Embrace beror på vem som använder tjänsten.

4. Brottsdatadirektivet, som genomförts i Sverige genom en ny brottsdatalag, är tillämplig enbart på myndigheter med brottsbekämpande uppdrag eller som utövar myndighet samt andra aktörer med motsvarande uppdrag. En tydlig målgrupp för Embrace är bl.a. kommuner och Polismyndigheten.

5. Kommuner har inte ett brottsbekämpande uppdrag eller utövar myndighet för de syften som brottsdatadirektivet anger. När kommunerna använder Embrace ska de således iaktta dataskyddsförordningens och dataskyddslagens bestämmelser.

6. Polismyndigheten däremot ska beakta polisdatalagens bestämmelser när myndigheten använder Embrace, och därutöver brottsdatalagen. I nuläget bedöms polisens personuppgiftsbehandling ha stöd i den nuvarande polisdatalagens bestämmelser. Den 1 januari 2019 träder en ny lag om polisens behandling av personuppgifter inom brottsdatalagens område i kraft. Den preliminära bedömningen är dock att personuppgiftsbehandlingen i Embrace inom ramen för polisens brottsförebyggande arbete alltjämt kommer att vara tillåten enligt lagen om polisens behandling av personuppgifter inom brottsdatalagens område.

7. Embraces kunder är *personuppgiftsansvariga* för sin användning av personuppgifter i tjänsten, t.ex. kommuner, Polismyndigheten samt bostads- och fastighetsföretag. Det beror på att Embrace är en molntjänst. Var och en av kunderna ansvarar också för sina uppgifter som man tillför den gemensamma lokala problembilden i Embrace Insight. Embrace Safety AB hanterar personuppgifter, i de fall sådana förekommer i tjänsten, i rollen som personuppgiftsbiträde. Personuppgiftsbiträden har ett begränsat juridiskt ansvar för de personuppgifter man behandlar i rollen som personuppgiftsbiträde. Bl.a. får bolaget ett självständigt ansvar för att säkerställa skyddet för eventuella personuppgifter i tjänsten samt rapportera personuppgiftsincidenter utan onödigt dröjsmål till sina kunder.

8. Inom en kommun är alltid en nämnd eller kommunstyrelsen personuppgiftsansvarig. Beträffande osjälvständiga nämnder, t.ex. utförarnämnder av viss verksamhet eller IT, är ofta en annan, självständig nämnd personuppgiftsansvarig för den osjälvständiga nämndens personuppgiftsbehandling. Embrace Safety AB bör vara uppmärksam på detta förhållande när personuppgiftsbiträdesavtal ska tecknas med en förvaltning/nämnd som vill använda Embrace. Det är ett krav enligt dataskyddsförordningen och brottsdatalagen att ett skriftligt personuppgiftsbiträdesavtal ska tecknas när en aktör behandlar personuppgifter för en personuppgiftsansvarigs räkning.

9. Det är de personuppgiftsansvariga, dvs. Embrace Safetys AB:s kunder, som ska iaktta de grundläggande principerna för dataskydd i dataskyddsförordningen respektive brottsdatalagen vid all personuppgiftsbehandling i Embrace, men det utesluter inte att Embrace Safety AB erbjuder stöd och utformar tjänsten så att kunderna kan leva upp till dataskyddsprinciperna. Om personuppgifter behandlas med stöd av en rättslig grund, men någon av de grundläggande dataskyddsprinciperna inte är iakttagna, riskerar personuppgiftsbehandlingen att betraktas som otillåten.

10. Kommuner ansvarar enligt författning för ett flertal verksamheter som har brottsförebyggande effekt. Kommuner har vidare en nyckelroll i regeringens nya nationella brottsförebyggande program – *Tillsammans mot brott* (2017). Polisen är beroende av kommunerna för sin brottsförebyggande verksamhet.

11. Mot den bakgrunden får kommuner lagligen behandla personuppgifter i Embrace, i de fall sådana förekommer i tjänsten, för att det är nödvändig för att kunna *utföra en arbetsuppgift av allmänt intresse* (art. 6.1 e dataskyddsförordningen samt 2 kap. 4 § dataskyddsförordningen). Kommunen behöver således inte inhämta ett samtycke av enskilda personer i de fall deras personuppgifter behandlas i Embrace.

12. För flertalet uppgifter i kommunens egen instans av Embrace råder ingen sekretess eftersom de inte kan hänföras till någon individ utan enbart till en plats. Sådana uppgifter kan utan risk för men eller skada för enskilda fysiska personer göras tillgängliga i den gemensamma, lokala problembilden i Embrace (Embrace Insight), t.ex. för Polismyndigheten samt bostads- och fastighetsbolag. Även för händelser kopplade till adress- och fastighetsuppgifter i Embrace bedöms risken som liten för men eller skada för enskilda fysiska personer, och uppgifterna borde som regel kunna lämnas ut till den gemensamma problembilden utan hinder av sekretess. Det är emellertid varje kommunal nämnds ansvar att beakta tillämpliga sekretessbestämmelser.

13. Polismyndigheten bedöms kunna, som nämnts (se punkt 6), behandla personuppgifter i Embrace, i de fall sådana uppgifter förekommer i tjänsten, med stöd av polisdatalagen, kompletterad av brottsdatalagen. Polisen bedöms vidare med stöd av polisdatalagen lagligen få behandla personuppgifter i den egna instansen av Embrace för att lämna ut dem till den gemensamma problembilden i Embrace (Embrace Insight), där andra samverkande, behöriga aktörer, t.ex. myndigheter (kommuner), kan ta del av uppgifterna. Även privata aktörer, t.ex. bostads- och fastighetsbolag, kan vara mottagare av sådana uppgifter med stöd av polisdatalagen (2 kap. 8 § 4 stycket). Utlämnandebehandlingen bedöms – inom ramen för ett lokalt brottsförebyggande arbete för vilket Embrace används - inte vara oförenlig med de ändamål för vilka polisen ursprungligen samlar in uppgifterna, t.ex. genom brottsanmälningar.

14. I Embrace finns, som nämnts, inga individuppgifter utan endast uppgifter om platser. Sådana uppgifter bedöms utan hinder av tillämpliga sekretessbestämmelser kunna lämnas ut av polisen till den gemensamma lokala problembilden i Embrace (Embrace Insight), där bl.a. kommuner samt bostads- och fastighetsbolag kan ta del av uppgifterna. Utlämnande kan i tveksamma fall, främst beträffande händelser i polisens egen instans av Embrace som är kopplade till uppgifter om gatu- och fastighetsadresser, ske med stöd av antingen ett ”nödvändigt utlämnande” (10 kap. 2 § offentlighets- och sekretesslagen) eller efter en intresseavvägning enligt den s.k. generalklausulen i 10 kap. 27 § i samma lag, oavsett om mottagaren är en icke brottsbekämpande myndighet eller privat aktör, vilka samverkar med polisen i det brottsförebyggande arbetet på lokal nivå.

15. Användare inom näringslivet bedöms lagligen kunna behandla personuppgifter, i de fall sådana förekommer i Embrace, efter en *intresseavvägning* (art. 6.1 f dataskyddsförordningen). Bostads- och fastighetsföretag hör klart till den kategorin och får anses ha ett berättigat intresse av att behandla personuppgifter i Embrace med hänsyn till deras påverkansmöjligheter för en trygghetsskapande miljö, varvid intresset för att skydda enskilda personliga integritet får ge vika. Bostadspolitiken är vidare ett fokusområde i regeringens nya nationella brottsförebyggande program (se punkt 10). Något samtycke behövs således inte om personuppgiftsbehandlingen i Embrace sker med den lagliga grunden ”intresseavvägning”. Andra privata aktörer måste göra en egen laglighetsprövning av Embrace och utröna den lagliga grunden för personuppgiftsbehandling. Kommunala bostads- och fastighetsbolag är inte myndigheter i lagens mening, men kan åberopa samma lagliga grund som kommunen, dvs. utförande av ”arbetsuppgifter av allmänt intresse” (6.1 e dataskyddsförordningen) eftersom dessa bolag lyder under kommunal styrning och tillhandahållande av bostäder är av allmänt intresse.,

16. Embrace innehåller inte, och ska inte innehålla *känsliga personuppgifter*, t.ex. uppgift om etnicitet, religionstillhörighet eller hälsa. Sådana uppgifter kräver särskilda lagliga grunder för registrering. Det erinras dock att Embrace har fritextrutor. I fritextrutorna så öppnar Embrace upp för registrering av sådana uppgifter. Ett alternativ är att ta bort fritextrutorna helt och hållet. Ett annat alternativ är att bygga in mekanismer i Embrace som förhindrar sådan registrering. I nuläget finns – såvitt kan bedömas – godtagbara tekniska och administrativa funktioner på plats i Embrace som ska förhindra att individuppgifter och känsliga personuppgifter förekommer hos de enskilda användarna eller lämnas ut till den gemensamma lokala problembilden.

17. I Embrace registreras som regel händelser om vad, var, när och åtgärd. Bilder kan också registreras, men enbart med syfte att följa upp insatser på platser som

är särskilt drabbade av brottsrelaterade händelser och andra otrygghetsskapande händelser. Det kan röra sig om bilder på klotter eller annan skadegörelse samt förändringar i miljön som vidtagits för att undvika klotter. Bilder och fotografier kan utgöra personuppgifter om man kan härleda dessa direkt eller indirekt till en fysisk levande person. Ibland kan en bild, t.ex. ett fotografi av klotter, röja vem som står bakom klottret. Klotter är en form av brottslig skadegörelse, och därmed uppstår en situation där personuppgifter behandlas om inte enbart en brottslig gärning utan dessutom en känd gärningsman. Enligt artikel 10 dataskyddsförordningen är det förbjudet för andra än myndigheter att behandla personuppgifter om fällande domar i brottmål och överträdelser (lagöverträdelser).

18. Förbudet för andra än myndigheter att behandla uppgifter om lagöverträdelser m.m. i artikel 10 i dataskyddsförordningen aktualiseras främst för de användare av Embrace som finns inom *näringslivet*, t.ex. bostads- och fastighetsföretag. Förbudet bedöms dock inte vara tillämplig på majoriteten av uppgifter som registreras som text eller bild i Embrace av dessa privata aktörer. Skälet är att förbudet torde ta fasta på uppgifter *om den som begått ett brott* och inte uppgifter om brottsoffer. En bild på en krossad glasruta på en viss fastighet samt registrering av gatuadressen träffas i normalfallet således inte av förbudet i artikel 10 eftersom det *inte* rör sig om behandling av personuppgifter om lagöverträdelser.

19. Fotografier av klotter och annan skadegörelse av vilka framgår kännetecken för en viss gärningsmans arbetssätt, s.k. modus operandi, vid brott riskerar däremot att träffas av förbudet i artikel 10 dataskyddsförordningen. Embrace Safety AB rekommenderas därför att informera och utbilda sina privata kunder att de inte får registrera digitala bilder som utvisar vem gärningsmannen är, t.ex. taggar på bilder på klotter eller ett modus operandi. Redan i dag har emellertid Embrace sådan utbildning samt tekniska och administrativa funktioner på plats i tjänsten som ska förhindra att individuppgifter alternativt känsliga personuppgifter registreras i Embrace. Embrace Safety AB rekommenderas att friskriva sig från allt ansvar för dessa kunders registrering av digitala bilder som utvisar vem som har begått ett brott.

20. Embrace Safety AB bör informera och utbilda kommuner och polisen om att de inte får dela bilder i Embrace Insight (den gemensamma lokala problembilden) med privata användare som utvisar vem som begått ett brott. En sådan delning kan vara straffbar. Även i detta fall rekommenderas Embrace Safety AB att implementera mekanismer i själva tjänsten som förhindrar sådan informationsöverföring till privata aktörer.

21. Alla aktörer som använder Embrace har en informationsskyldighet mot registrerade. Vilken information som ska lämnas framgår av dataskyddsförordningen, brottsdatalagen och polisdatalagen. Information ska som huvudregel lämnas skriftligen, men kan också lämnas i annan form inklusive elektronisk form. Information om Embrace kan således lämnas genom etablerade kommunikationskanaler med invånare och hyresgäster, t.ex. genom nyhetsbrev, e-postutskick, annonsering i lokaltidning i kombination med information på en hemsida. Det centrala är att informationen når samtliga som kan komma att beröras av registreringen i Embrace. Det är viktigt att det finns dokumenterade rutiner för informationsskyldigheten och att exempelvis nyinflyttade personer nås av informationen.

Innehåll

1 Inledning

Embrace är en digital tjänst avsedd för brottsförebyggande lokal samverkan, t.ex. mellan polis, kommun och näringslivet. Embrace gör det möjligt att bedriva sådan samverkan både på ett kunskapsbaserat och metodiskt sätt. En central funktion i Embrace är den gemensamma lokala problembilden (Embrace Insight). Det är en bild av var och när saker sker och hur utvecklingen över tid ser ut. Alla lokalt samverkande parter som använder Embrace bidrar med information till den gemensamma problembilden, och kan ta del av densamma. Metoden som används i Embrace bygger på en metod som förespråkas av Brottsförebyggande rådet (Brå), Polismyndigheten och Sveriges Kommuner och Landsting (SKL) vid lokalt brottsförebyggande arbete.[1] Embrace utvecklas av Embrace Safety AB i samverkan med bl.a. Polismyndigheten och ett flertal kommuner.

Den övergripande frågan som ska besvaras i denna promemoria är i vilken utsträckning personuppgifter behandlas, och får lagligen behandlas i Embrace, och av vem (laglighetsprövning).

En laglighetsprövning kan i flera avseenden beskrivas som en process för att identifiera eller hantera juridiska risker. Den övergripande risken vid personuppgiftsbehandling är att inte iaktta bestämmelser om persondataskydd. Persondataskyddet består av dels sekretess- och tystnadspliktsbestämmelser, dels registerförfattningar. Bestämmelser om sekretess och tystnadsplikt finns i offentlighets- och sekretesslagen (2009:400) och andra författningar. Behandling av personuppgifter regleras i EU:s dataskyddsförordning, lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) samt i ett flertal olika registerförfattningar beroende på huvudman eller verksamhet. Vid behandling av personuppgifter för brottsutredande syften gäller brottsdatalagen (2018:1177) i stället för dataskyddsförordningen.

Den som obehörigen röjer personuppgifter i strid med lagstadgad sekretess- och tystnadsplikt riskerar böter eller fängelse. Underlåtenhet att uppfylla författningsenliga krav för behandling av personuppgifter kan medföra skadestånd och kraftfulla administrativa vitessanktioner. Mot den bakgrunden är en juridisk riskanalys nödvändig för att kunna fastställa om t.ex. insamling av brottsrelaterade uppgifter, fortsatt behandling och utlämnande av dessa till annan aktör är tillåtet eller inte enligt gällande rätt.

En laglighetsprövning motiveras också av andra skäl. Rättsreglerna förutsätter ofta att någon form av juridisk riskanalys genomförs. Inte minst mot bakgrund av att

[1] Se Samverkan i lokalt brottsförebyggande arbete, utgiven av Brå, Polismyndigheten och SKL 2016. I publikationen beskrivs ett kunskapsbaserat arbetssätt i en så kallad samverkansprocess med hjälp av samverkansöverenskommelser och medborgarlöften.

författningar lätt kan halka efter samhällsutvecklingen. Beträffande IT måste rättsreglerna normalt sett också åtlydas även under en pilotdrift eller testverksamhet som innefattar personuppgifter. Rättsreglernas auktoritativa natur innebär vidare att juridiken i sig kan utgöra en risk i det att underlåtenhet att beakta det juridiska regelverket i utvecklingsfasen kan medföra negativa konsekvenser vid en kommersialisering eller bred implementering av lösningen eller innovationen.

Genom en laglighetsprövning identifieras således risker, vilka kan reduceras eller elimineras genom tekniska, organisatoriska eller administrativa åtgärder.

Dataskyddsförordningen ställer bl.a. krav på den personuppgiftsansvarige att i vissa fall genomföra *dataskyddskonsekvensbedömningar* (artikel 35). Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en *hög risk för fysiska personers rättigheter och friheter* ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En konsekvensbedömning är alltid obligatorisk vid hantering i stor omfattning av särskilda kategorier av personuppgifter eller av personuppgifter som rör fällande domar.

Föreliggande utredning utgör inte en dataskyddskonsekvensbedömning. Det är en laglighetsprövning, dvs. en bedömning huruvida den planerade personuppgiftsbehandlingen är laglig eller inte, och vilka åtgärder som ska vidtas för att säkerställa regelefterlevnad och därmed minska risken för att fysiska personers rättigheter och friheter kränks. En konsekvensbedömning ska bl.a. innehålla ”de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs”. Denna laglighetsprövning redovisar inte risker i tekniska lösningar, system eller utrustning. Den kan emellertid utgöra ett led eller underlag för en konsekvensbedömning enligt dataskyddsförordningen.

Laglighetsprövningen innehåller en beskrivning av Embrace, frågeställningar, juridiska överväganden och rekommendationer till Embrace Safety AB.

Rättsutredningen har utförts av Manólis Nymark (Manolis Nymark Consulting) på uppdrag av Örebro Universitet Enterprise AB.

I en bilaga (bilaga 1) finns en redogörelse för centrala begrepp i utredningen.

2 Bakgrund

I detta kapitel lämnas en redogörelse för bakgrunden till laglighetsprövningen och den digitala tjänsten Embrace.

2.1 All brottslighet sker lokalt och kan därför förebyggas lokalt

Brottslighet är inte slumpmässig utan uppträder enligt vissa mönster. Statistik visar att vissa hus är mer utsatta för inbrott än andra, och att vissa personer är mer utsatta för våldsbrottslighet än andra.[2] Med sådan kunskap kan brottsförebyggande åtgärder effektivare riktas mot brottsproblemen.

Det är polisen som har till huvuduppgift att minska brottsligheten i samhället och öka allmänhetens och näringslivets trygghet. Även andra myndigheter arbetar mer eller mindre brottsförebyggande, bl.a. kommunerna. Kommunerna har en mängd ansvarsområden som har en brottsförebyggande effekt och tillhandahåller olika välfärdstjänster som syftar till att minska risken för utanförskap och förstärka känslan av anknytning till samhället.

Enligt Brottsförebyggande rådet (Brå) är samverkan mellan olika samhällsaktörer nödvändigt för ett effektivt brottsförebyggande arbete. Polis och kommun är två aktörer som nästan alltid berörs av sådan samverkan, men även näringsliv och andra aktörer, t.ex. bostadsbolag, kan bidra till det brottsförebyggande arbetet.

Den 1 januari 2015 fick Sverige en ny polisorganisation som ska utgå från det lokala perspektivet. Det innebär bland annat en höjd ambitionsnivå för samverkan mellan polis och kommun i brottsförebyggande frågor. Idag bedrivs lokalt brottsförebyggande arbete i nästan alla kommuner. Ofta bedrivs arbetet i brottsförebyggande råd där kommun och polis samarbetar utifrån lokala, gemensamma problembilder.

I vägledningen *Samverkan – i lokalt brottsförebyggande arbete*, utgiven av Polismyndigheten, Sveriges Kommuner och Landsting (SKL) och Brå, beskrivs den nuvarande samverkansmodellen mellan kommun och polis. Av vägledningen framgår hur denna samverkan ska bedrivas i olika steg. Samverkan ska ske enligt ett kunskapsbaserat arbetssätt i en så kallad samverkansprocess med hjälp av samverkansöverenskommelser och medborgarlöften.

[2] https://www.bra.se/forebygga-brott/arbeta-kunskapsbaserat.html

2.2 Embrace

För att hitta lokala lösningar för att förebygga brott och andra otrygghetsskapande händelser är det nödvändigt att arbetet baseras på kunskap om den lokala brottsligheten. Enligt Brå kan det lokala brottsförebyggande arbetet endast bli effektivt om de bedrivs mer kunskapsbaserat än vad som sker i dag.[3]

Det är bakgrunden till Embrace. Tjänsten stöder ett kunskapsbaserat och metodiskt arbetssätt i det lokala brottsförebyggande och trygghetsfrämjande arbetet. Metoden är densamma som i den samverkansmodell som förespråkas av Polismyndigheten, SKL och Brå (se föregående avsnitt) och bygger på ett flertal steg:

1. Kartläggning
2. Analys
3. Insats
4. Uppföljning
5. Återkoppling.

Med hjälp av Embrace kan parterna dokumentera, visualisera och analysera samtliga fem stegen.[4]

En central del i det lokala samverkande arbetet mot brott och andra otrygga händelser är att dela och komplettera varandras information (om brottsrelaterade och andra otrygghetsskapande händelser) i en så kallad gemensam lokal problembild. Det är en grafisk översiktsbeskrivning av var och när saker sker och hur utvecklingen över tid ser ut. Sekretessbelagd information, t.ex. uppgifter som omfattas av förundersökningssekretess, ska inte delas mellan samverkande parter. Embrace innehåller således en sådan lokal problembild (Embrace Insight) där lokalt samverkande parter kan dela med sig av sin information, och ta del av densamma.

Embrace innehåller också vägledningar i samtliga av dessa steg för att integrera tidigare forskning och annan kunskap (evidens) i exempelvis analysen eller besluten om vilka insatser som ska sättas in. Detta gör Embrace unikt. Andra liknande tjänster fokuserar mer på kartläggning och prediktion.

Embrace kan visualisera alla data som samlas in, både som grafer och på karta. Exempel på sådan data är

- polisanmälda brott,
- icke polisanmälda, men misstänkta brott
- rapporter om otrygghet, och
- karaktäristika för en specifik plats (t.ex. dålig belysning och få cykelställ).

I Embrace registreras både händelser samt insatser eller åtgärder för att försvåra eller förhindra en upprepning av en viss händelse. En viktig uppgift som ska registreras är platsen för ett brott eller en otrygghetsskapande händelse. Ett krossat fönster i ett bostadshus kan registreras på gatuadressen eller fastighetsadressen. Även GPS-koordinater kan registreras. Det kan användaren göra för att visa var på en

[3] https://www.bra.se/forebygga-brott/arbeta-kunskapsbaserat.html
[4] https://www.oru.se/forskning/forskningsprojekt/fp/?rdb=p1635

byggnad något har skett. Ibland vet man bara området och då registreras den uppgiften. Endast brottslighet i offentliga miljöer är i fokus, inte brott som sker i hemmet, dock inbrott, vilket ju sker utifrån. Som offentlig miljö räknas platser utomhus och även bl.a. köpcentra. Händelser i en bostad registreras aldrig. Gatu- och fastighetsadresser, liksom GPS-koordinater, är sökbara i Embrace.

Embrace registrerar inte enskilda individer. Människor är inte i fokus för det brottsförebyggande arbetet, varken brottsoffer eller förövare. Det är händelsen som är av intresse. Och, som nämnts, platsen för densamma.

Inte heller insatser eller åtgärder som registreras i Embrace är inriktade mot specifika individer. Som exempel på insatser kan nämnas sanering av klotter, polisanmälan, polispatrullering, bevakning, nattvandrare och förändringar i miljön (t.ex. uppsätta belysning, ta bort buskage m.m.). Även åtgärder eller insatser kan vara kopplade till en gatu- eller fastighetsadress, såsom ett lagat fönster eller en polisanmälan. Registrering av andra insatser som nattvandring och patrullering kan ske i form av platser, områden och centrumbyggnader, inte typiskt till hemadresser.

Embrace inrapporteringsverktyg (Embrace IQ) innehåller formulär och fritextrutor där händelser eller insatser kan beskrivas. Embrace Safety AB, som tillhandahåller tjänsten, utbildar användare att undvika registrering av individuppgifter i fritextrutorna. Skulle sådana uppgifter registreras ansvarar en anställd, tillika administratör, hos varje organisation för att ta bort sådana uppgifter. Uppgifter hos en organisation kan inte heller tekniskt lämnas ut till Embrace Insight (den lokala gemensamma problembilden) utan ett godkännande av behörig administratör.

Embrace rapportverktyg kan nås via mobila enheter så att registrering kan ske på plats.

Fotografier är en del av dokumentationen i Embrace. Med hjälp av fotografier kan insatser följas upp, t.ex. när en insats handlar om att förändra en miljö/plats. Fotografier används således inte för att dokumentera brottsrelaterade eller andra otrygghetsskapande händelser, men det utesluter inte fotografier av t.ex. skadegörelse av olika slag i syfte att följa upp insatser på platser som är särskilt utsatta för brottsrelaterade eller andra otrygghetsskapande händelser för att hindra sådant i framtiden.

Embrace är inte ett brottsutredande verktyg utan ett brottsförebyggande stöd. Informationsdelningen mellan dem som använder tjänsten, t.ex. polis och kommun, syftar inte till att gripa förövare utan att reducera eller eliminera de faktorer som inbjuder eller underlättar brottslig verksamhet.

Embrace kan berikas med information från andra kunskapskällor. Som exempel kan nämnas polisens eget rapportsystem, GPS-spårare på patrullerande ordningsvakter/nattvandrare och mobila enheter för bostadsvärdar. Även aggregerade uppgifter från SCB på områdesnivå kan läggas in i Embrace. Man kan också registrera önskemål från invånare om vilka aspekter polisen ska fokusera på inom ramen för s.k. medborgarlöften. Ett medborgarlöfte är ett åtagande gentemot

medborgarna som polis och kommun gör i samverkan, gärna även med andra samverkansparter.

Embrace planeras också att i framtiden kunna göra prediktioner eller prognoser var olika typer av brott har olika hög sannolikhet att ske den närmsta tiden och även var det kan förväntas vara otryggt. Embrace kan därmed användas som beslutsunderlag för brottsförebyggande och trygghetsfrämjande insatser.

All data som matas in i Embrace kan samanalyseras för att se hur åtgärder/insatser och karaktäristik har samband med brott och upplevd trygghet. Man kan se vilka insatser som verkar effektiva och vilka som inte verkar vara det. Embrace har också funktionalitet för olika slag av rapporter.

Embrace är användarvänligt i alla led, från inrapportering och skapande av projekt till analys och uppföljning.

Med hjälp av informationen och kunskapen om lokala brott i Embrace kan t.ex. både polis och kommun dela informationen till andra, t.ex. ideella föreningar som ska nattvandra och det brottsförebyggande rådet med representanter från det lokala näringslivet och lokalpolitiken. Redan idag är det brukligt att polisen visar brottsförebyggande rådets medlemmar i kommunen brottskartläggningar på karta, t.ex. misshandel i en park utomhus och cykelstölder vid en järnvägsstation med angivande av exakt geografisk position.

Embrace erbjuds som en molntjänst samt tillhandahålls och utvecklas av Embrace Safety AB. En arbetsgrupp bestående av personer från Örebro Universitet Enterprise AB och användare (t.ex. polis, kommun, bostadsföretag) deltar i utvecklingsarbetet.

En första version av tjänsten utvecklades och testades under 2016 inom ramen för ett Brå-finansierat projekt; Effektiv Samordning för Trygghet (EST).

3 Uppdragsbeskrivning och frågeställningar

I detta kapitel lämnas en redogörelse för uppdraget, problemställningar och de juridiska frågeställningar som ska besvaras.

3.1 Tillsammans mot brott

I juni 1996 presenterade regeringen sitt första brottsförebyggande program - Allas vårt ansvar (Ds 1996:59). Syftet var ett långsiktigt och uthålligt brottsförebyggande arbete inom alla samhällssektorer. Programmet kom att få stor betydelse för utvecklingen av det brottsförebyggande arbetet på lokal nivå, dvs. samverkan mellan Polismyndigheten och kommunerna. I och med ombildningen till en myndighet 2015 inrättades två nya funktioner i Polismyndigheten, områdespolis och kommunpolis, med syfte att skapa lokal förankring och arbeta främst brottspreventivt.

Brottsligheten har sedan 1996 förändrats. Av det skälet fann regeringen utöver de åtgärder som hittills har vidtagits inom ramen för den tidigare satsningen att 2017 lansera ett nytt brottsförebyggande program – *Tillsammans mot brott*.[5] Det riktar sig, i likhet med Allas vårt ansvar, till en bred målgrupp inom många samhällssektorer så att de brottsförebyggande frågorna får en mer framskjuten plats i samhället. För samordningen av programmet har regeringen utsett en nationell samordnare.

I regeringens brottsförebyggande program är kommunerna en nyckelaktör i det brottsförebyggande arbetet, men även många statliga myndigheter utanför rättsväsendet. I programmet uppmärksammar regeringen även näringslivets roll. Civila samhällets kunskap och erfarenhet ska tas tillvara i högre utsträckning. Forskares delaktighet ska bli en naturlig del i ett kunskapsbaserat arbete.

3.2 Situationell brottsprevention

I programmet beskriver regeringen olika modeller för att förebygga brott. En sådan är *situationell brottsprevention*.

Den mest tongivande modellen när det gäller polisens brottsförebyggande arbete är Problemorienterat polisarbete, (POP). Det är ett arbetssätt som bygger på att polisen, gärna i samverkan med andra, mycket noggrant kartlägger och analyserar de problem som ska hanteras. Förhoppningen är att denna analys ska ge uppslag till bättre och mer effektiva insatser.

Det problemorienterade arbetssättet har en brottsförebyggande inriktning, där polisen samarbetar med andra aktörer för att hitta och genomföra så bra lösningar på problemen som möjligt. I POP-perspektivet ingår också att effekten av de vidtagna

[5] Regeringens skrivelse 2016/17:126

insatserna ska utvärderas noga.[6] Analysen av de aktuella problemen kan inrymma orsaker och åtgärder både på individ-, grupp- och områdesnivå. Men inte sällan är de insatser som aktualiseras sådana som avser en specifik typ av brott och är inriktade mot den omedelbara situationen.

Det handlar inte om att åtgärda individuella eller strukturella orsaker utan om att minska tillfällena till brott.[7] Den typen av insatser brukar benämnas situationell brottsprevention. Metoden utesluter dock inte påverkan av gruppers brottsbenägenhet. Dessa insatser är sådana som polisen sällan själv kan vidta, utan det är andra myndigheter som ansvarar för dem. Eftersom det rör sig om lösningar för att förebygga brottsproblem initieras de dock ofta av polisen.

Analyser utifrån situationell brottsprevention kan ge uppslag till insatser. I litteraturen om situationell brottsprevention ges olika uppslag om hur man kan tänka när man analyserar möjliga insatser mot en typ av brott. Metoderna som används vid situationell brottsprevention brukar till exempel delas in i följande olika kategorier:[8]

- försvåra genomförandet av brott
- öka upptäcktsrisken
- minska vinsten av brott
- försvåra bortförklaringar
- reducera provokationer som kan leda till våld.

3.3 Andra brottsförebyggande modeller

En annan modell som regeringen beskriver i det nationella brottsförebyggande programmet Tillsammans mot brott handlar om förebyggande arbete riktat mot förutsättningar som krävs för att ett brott ska uppstå, vilket beskrivs i den s.k. *rutinaktivitetsteorin*. Denna bygger på att tre huvudsakliga faktorer måste vara uppfyllda för att ett brott ska kunna uppstå:

- En motiverad gärningsperson
- Ett lämpligt objekt eller offer för den kriminella handlingen
- Avsaknad av formell och informell kontroll, t.ex. låg risk att bli upptäckt eller svaga sociala band

Om någon av de tre förutsättningarna saknas minskar sannolikheten för att ett brott ska begås. Detta kan vändas till förebyggande åtgärder genom att antingen

1. minska motivationen hos en person att begå brott,
2. stärka den formella och informella kontrollen, dvs. öka upptäcktsrisken eller stärka andra faktorer som ökar den informella kontrollen
3. begränsa tillgängligheten till eller stärka skyddet av lämpliga brottsobjekt eller brottsoffer.

---

[6] Brå-rapport 2016:20. Insatser mot brott och otrygghet i socialt utsatta områden - En kunskapsöversikt, s. 11.
[7] Ib.
[8] Ib.

3.4 Brottsförebyggande aspekter i fysisk planering och bostadsbyggande

I det nationella brottsförebyggande programmet Tillsammans mot brott ägnar regeringen särskild uppmärksamhet åt brottsförebyggande aspekter i fysisk planering och bostadsbyggande.

Enligt prognoser från Boverket finns det behov av över 700 000 bostäder fram till 2025. Det är därför viktigt enligt regeringen att brottsförebyggande aspekter i högre grad beaktas i fysisk planering och bostadsbyggande och blir en naturlig del i byggprocessen. Det kan handla om allt från hur bostadsområden, parker och torg planeras och utformas till byggnadstekniska detaljer som lås, entréers utformning och belysning. Säkerhets- och trygghetsfrågorna måste vara en naturlig del i byggprocessen, anser regeringen.

Regeringen nämner konceptet BoTryggt som sedan 2016 förvaltas och utvecklas av Stiftelsen Tryggare Sverige med målet att skapa en uppdaterad standard inom området. BoTryggt syftar till att utifrån aktuell forskning och beprövad erfarenhet sprida kunskap om hur olika aktörer kan förebygga brott och öka tryggheten i bostäder och bostadsområden genom det fysiska rummets utformning.

Fastighetsföretagen är ett annat exempel på aktörer som kan arbeta brottsförebyggande. Regeringen skriver att det kan handla om att stötta grannsamverkan i flerbostadshus, trygghetsvandringar, nattvandrare och utformning av parker och gångstråk. I detta arbete krävs oftast ett samarbete med andra lokala aktörer. Business Improvement Districts (BID) är en internationell term som ännu saknar ett svenskt namn och som innebär att fastighetsägare tillsammans med boende och offentliga aktörer lyfter ett område genom bland annat investeringar i den offentliga miljön, fastigheter och i trygghetsskapande åtgärder. BID-inspirerad samverkan har successivt växt fram på några håll i Sverige. Med denna samverkansmodell menar regeringen skapas en sammanhållning även i större städer och bidrar till såväl ökad trygghet och säkerhet som attraktionskraft för företag och en ökad livskvalitet i stort.

Regeringen berör vidare teorin om ”Broken Windows”. Den går ut på att mindre allvarlig brottslighet som klotter och skadegörelse kan leda till allvarligare kriminalitet och otrygghet i ett område om det inte åtgärdas snabbt. Ett krossat fönster leder till fler krossade fönster, på samma sätt som en redan nerklottrad vägg drar till sig mer klotter. Omvänt innebär detta att en plats som är hel och ren bidrar till att minska brottsligheten. Åtgärderna bidrar också till att visa att området har social sammanhållning och stabilitet och att stärka känslan av att området är omhändertaget, med invånare som bryr sig om varandra. Insatser med detta som utgångspunkt bör vara enligt regeringen en del av det lokala brottsförebyggande arbetet. Här spelar, anser regeringen, kommunen en viktig roll, inte minst i egenskap av fastighetsägare och ansvarig för många offentliga platser. Även för landstingen, i egenskap av huvudman för kollektivtrafiken där mycket skadegörelse och klotter förekommer, kan denna strategi ha betydelse.

Regeringen deklarerar således att den bl.a. ska verka för

- att kunskap om situationellt brottsförebyggande arbete sprids till fler aktörer,
- att brottsförebyggande aspekter i högre grad beaktas i fysisk planering och bostadsbyggande, och
- att stötta samverkan mellan privata och offentliga aktörer som vill samverka kring lokala trygghetsfrågor.

3.5 Kunskapsbaserat arbete med kontinuerlig uppföljning och utvärdering

Forskning pekar på att den mest grundläggande förutsättningen för att bedriva ett effektivt brottsförebyggande arbete är att det i så hög grad som möjligt är kunskapsbaserat. En bra struktur för ett kunskapsbaserat arbete beskrivs i vägledningen *Samverkan - i lokalt brottsförebyggande arbete* som tagits fram av Brå, Polismyndigheten och Sveriges Kommuner och Landsting. Även regeringen framhåller i sitt sjösatta nationella brottsförebyggande program betydelsen av att brottsutredande och brottsförebyggande arbete bedrivs kunskapsbaserat, något som inte alltid varit fallet.

Att arbeta kunskapsbaserat innebär att strukturerat och systematiskt kartlägga och analysera aktuella förhållanden och förutsättningar, vilket inkluderar både problem, risker och möjligheter. För att identifiera brottsproblem, utsatta områden eller grupper kan det krävas statistik, expertkunskap, trygghetsmätningar och andra studier.

Utifrån en kartläggning och orsaksanalys bör relevanta åtgärder identifieras, prioriteras och beslutas. Åtgärderna bör sedan löpande följas upp och utvärderas. Det är också viktigt att arbetet dokumenteras och att resultatet av uppföljning och utvärdering används i det fortsatta utvecklingsarbetet.

Brå har konstaterat att det finns stora brister inom det här området, såväl på lokal nivå som på nationell nivå.[9] Många åtgärder vidtas utan att vara kunskapsbaserade eller baserade på den lokala problembilden och orsaksanalysen hoppas ofta över. Systematisk dokumentation av utvärderingar och uppföljningar av brottsförebyggande åtgärder behöver också utvecklas för att kunna utgöra ett underlag för beslut om prioriteringar när det gäller brottsförebyggande arbete inom den offentliga verksamheten.

För att möjliggöra en tydligare resultatredovisning på bl.a. lokal nivå har regeringen gett Polismyndigheten i uppdrag att utveckla sin verksamhetsuppföljning.[10] Uppföljningen av Polismyndighetens verksamhet ska framöver kunna redovisas på samtliga nivåer inom myndigheten, från nationell nivå till lokal nivå. Regeringens förstärkta struktur för stöd och samordning på nationell och regional nivå utgör också ett viktigt bidrag för att utveckla berörda aktörers förmåga att arbeta kunskapsbaserat.

[9] Skr. 2016/17:126 s. 26.
[10] Ib.

3.6 Embrace – ett verktyg för regeringens brottsförebyggande mål

Det råder ingen tvekan om att förebyggande av brott är en angelägenhet som berör hela samhället och att ingen kan stå utanför det arbetet. Brottsförebyggande arbete kan inte enbart framgångsrikt bedrivas av Polismyndigheten, utan kräver aktivt engagemang av andra samhällsaktörer, däribland kommuner samt bostads- och fastighetsbolag.

Embrace är utvecklat för att råda bot på de brister som hittills vidlåtit brottsförebyggande arbete på lokal nivå, nämligen vidtagande av åtgärder utan närmare analys av mönster, trender och orsakssamband. Embrace syftar till att ge stöd för att kunna arbeta evidensbaserat och systematiskt i det lokala situationella brottsförebyggande och trygghetsfrämjande arbetet. Strukturen i Embrace följer den process som både Brå och internationell forskning förespråkar för lokalt evidensbaserat brottsförebyggande och trygghetsskapande arbete.

Embrace har därför rönt stort intresse inte hos bara polisen utan även hos andra aktörer som i regeringens brottsförebyggande program utpekas som viktiga för det brottsförebyggande arbete, t.ex. kommuner, bostads- och fastighetsbolag, landsting (kollektivtrafiken) och övrigt näringsliv.

3.7 Problembild

Som redovisats är Embrace inte ett verktyg för att utreda och lagföra brott. Embrace registrerar inte enskilda individer utan enskilda händelser på en detaljerad nivå. Detaljeringsnivån väcker dock frågor om Embrace hanterar *personuppgifter* per definition. I sådant fall ska bestämmelser om dataskydd iakttas av de aktörer som använder Embrace. Sådana bestämmelser finns först och främst i EU:s dataskyddsförordning och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Därutöver finns i Sverige omkring 200 särskilda registerförfattningar, varav polisdatalagen (2010:361) är ett sådant exempel. Polisdatalagen upphör den 1 januari 2019 och ersätts av lagen om polisens behandling av personuppgifter inom brottsdatalagens område.[11]

Behandling av personuppgifter relaterade till brott och lagföring utgör en särskild kategori av personuppgifter som lagstiftaren anser ska behandlas med försiktighet och endast av aktörer som har ett berättigat intresse. Till den kretsen hör normalt sett inte privatpersoner eller företag. Enligt artikel 10 dataskyddsförordningen är det förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, fällande dom i ett brottmål och straffprocessuella tvångsmedel, t.ex. häktning, reseförbud eller beslag.[12] Behandling av personuppgifter i den brottsbekämpande verksamheten regleras i brottsdatalagen (2018:1177). Lagen ska alltså tillämpas i stället för

[11] Lagen har i skrivande stund inte publicerats i svensk författningssamling. Regeringens förslag till lagen finns i prop. 2017/18:269.
[12] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/kansliga-personuppgifter/personuppgifter-som-ror-lagovertradelser/

dataskyddsförordningen Frågan är således om Embrace hanterar de facto ”personuppgifter” i dataskyddsförordningens mening, och om de händelser som registreras faller in under förbudet i artikel 10 dataskyddsförordningen. Det skulle innebära att enbart myndigheter kan använda Embrace, vilket skulle kraftigt begränsa inte bara tjänstens nytta utan också regeringens ambitioner på det brottsförebyggande området, t.ex. att bedriva ett kunskapsbaserat brottsförebyggande arbete som involverar näringslivet (se avsnitt 3.1).

Faktum är att regeringens rättspolitiska program med ambitionen att bedriva det brottsförebyggande arbetet kunskapsbaserat och metodiskt riskerar att undergrävas av lagstiftarens högt ställda krav på persondataskydd. Någon analys verkar inte ha gjorts av regeringen kring denna problembild för det nya brottsförebyggande programmet *Tillsammans mot brott*. Vidare, om Embrace behandlar personuppgifter, måste den lagliga grunden för sådan personuppgiftsbehandling fastställas.

3.8 Uppdrag och frågeställningar

Föreliggande laglighetsprövning utgör ett led i utvecklingen av Embrace. Den övergripande frågan som ska besvaras är i vilken utsträckning personuppgifter behandlas, och får behandlas lagligen i Embrace, och av vem.

Laglighetsprövningen tar sin utgångpunkt i dataskyddsförordningen och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Den nya regleringen innebär inte att tidigare praxis från domstolar och Datainspektionen saknar helt relevans. Av skäl 9 i dataskyddsförordningen framgår nämligen att målen och principerna för det tidigare dataskyddsdirektivet, som låg till grund för personuppgiftslagen, är fortfarande giltiga. Även sekretess- och tystnadspliktbestämmelser ska beaktas.

Centrala frågor som ska besvaras är följande:

- Behandlar Embrace personuppgifter eller inte?
- Får rapportering, inklusive fotografering av skadegörelse på skolor, bostäder och kommersiella fastigheter registreras i Embrace, t.ex. klotter?
- Om Embrace behandlar personuppgifter, med vilken laglig grund får det ske, t.ex. registrering av adressuppgifter?
- Omfattar förbudet i 21 § personuppgiftslagen enbart uppgifter om förövaren, men inte uppgifter om brottsoffren?
- Om enbart myndigheter får behandla personuppgifter i Embrace, hör nämnder i kommuner till den kategorin av myndigheter?
- Får en privat aktör, exempelvis ett kommunalt bostadsbolag, behandla personuppgifter rörande förövaren respektive brottsoffret i Embrace om det finns en samverkan med en myndighet, t.ex. polisen?
- Får en myndighet dela information i Embrace med privata aktörer, t.ex. att polisen delar information om händelser med ett kommunalt bostadsbolag, under förutsättning att det finns en samverkan mellan bostadsbolaget och polisen?

Klargörande efterfrågas vidare av följande frågeställningar:

- Är RPSFS 2012:18, Rikspolisstyrelsens föreskrifter och allmänna råd till lagen (1974:191) och förordningen (1989:149) om bevakningsföretag tillämplig på Embrace, dvs. om den aktör som använder Embrace rent formellt måste ha auktorisation från länsstyrelsen eftersom det rör sig om en verksamhet som syftar till förbättrat skydd?

3.9 Avgränsningar

Utredningen är avgränsad till ovan nämnda frågeställningar.

4 Gällande rätt

Skyddet för privatlivet och den personliga integriteten vid behandling av personuppgifter finns i dataskyddsförordningen, lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och i ett flertal s.k. registerförfattningar. Det finns i dagsläget omkring 200 registerförfattningar. Med ”personuppgifter” avses enligt dataskyddsförordningen varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet (art. 4.1).

Från dataskyddsförordningens tillämpningsområde undantas bl.a. personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straff, inkluderande skydd mot samt förebyggande av hot mot den allmänna säkerheten. Den personuppgiftsbehandling som görs för dessa syften faller i stället under ett nytt dataskyddsdirektiv om skydd för enskilda personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder (brottsdatadirektivet). Till skillnad från dataskyddsförordningen, som gäller direkt i varje medlemsland, ska brottsdatadirektivet genomföras i varje medlemsland genom nationell reglering. Direktivet har i Sverige genomförts genom en ny brottsdatalag (2018:1157; se kapitel 7).

Bestämmelser om dataskydd syftar till att balansera skyddet för den personliga integriteten mot vissa angelägna samhällsintressen där skyddet måste få vika. Det är en balansgång som inte alltid är given och som ofta blir föremål för tolkningar. Dataskyddsförordningen, brottsdatalagen och övriga registerförfattningar utgör en väsentlig del av det s.k. persondataskyddet. Hit hör även bestämmelser om sekretess- och tystnadsplikt.

Embrace är avsett för brottsförebyggande syften. Hanterar Embrace personuppgifter per definition är en avgörande fråga vilken reglering, brottsdatalagen eller dataskyddsförordningen, som är tillämplig på tjänsten.

Uppgifter om brott omfattas av en särreglering i dataskyddsförordningen. Sådana personuppgifter omfattas som inte av definitionen i artikel 9.1 dataskyddsförordningen för känsliga personuppgifter, men de berör ändå känsliga förhållanden. Därför finns det särskilda restriktioner i fråga om vilka personuppgiftsansvariga som får behandla sådana uppgifter. Det är enligt artikel 10 dataskyddsförordningen förbjudet för andra än myndigheter att behandla sådana personuppgifter om lagöverträdelser som innefattar brott, fällande domar i brottmål,

straffprocessuella tvångsmedel, t.ex. häktning, reseförbud och beslag. Det är dock oklart om misstanke om brott ska hänföras till kategorin personuppgifter om lagöverträdelser.[13] Förbudet behöver dock inte beaktas vid sådan behandling av personuppgifter som sker för forskningsändamål. Samtycke får dock inte användas för att göra undantag från förbudet.

När man som i detta fall vill registrera händelser som kan vara relaterade till brott i Embrace måste aktuellt regelverk iakttas. Man brukar i dessa sammanhang tala om en *laglighetsprövning*.

Denna rättsutredning syftar till att just göra en sådan laglighetsprövning. Av det skälet lämnas i detta kapitel en orientering om gällande rätt. I kapitel 5 och 6 lämnas därför en redogörelse för dataskyddsförordningen respektive brottsdatadirektivet. I kapitel 7 lämnas en redogörelse för brottsdatalagen. I samma kapitel lämnas också en orientering om dataskyddslagen.

4.1 Grundläggande bestämmelser om skyddet för den personliga integriteten

I Sverige, liksom i många andra rättsstater, bygger regleringen av enskildas fri- och rättigheter på dels en nationell grundlagsreglering, dels folkrätten och dels ingångna internationella avtal. I sistnämnda hänseende intar för Sveriges del EU-rätten principiellt sett en särställning, eftersom denna inom sitt tillämpningsområde i händelse av normkonflikt har företräde framför nationell rätt.

Även Europakonventionen har en särställning genom att den inte bara har gjorts till en integrerad del av den svenska rättsordningen utan också föranlett ett grundlagsstadgat förbud mot lagstiftning i strid med Sveriges åtaganden enligt konventionen.

Regeringsformen (RF) är en grundlag som innehåller bestämmelser om Sveriges statsskick. I 2 kap. behandlas de grundläggande fri- och rättigheterna. Där tillförsäkras medborgarna vissa fri- och rättigheter som har särskild betydelse för politisk och liknande verksamhet, såsom yttrandefrihet, informationsfrihet, mötesfrihet, demonstrationsfrihet, föreningsfrihet och religionsfrihet.

RF innehåller vidare bestämmelser till skydd för den enskildes personliga frihet och säkerhet. Enligt 2 kap. 6 § andra stycket RF är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Detta grundlagsskydd omfattar även vissa mer ingripande integritetsintrång från det allmännas sida som sker genom automatiserad behandling av personuppgifter. Begränsningar av grundlagsskyddet måste enligt 2:20 1 st. RF göras genom lag.

Dataskyddsförordningen respektive brottsdatalagen är sådana begränsningar av grundlagsskyddet. Lagarna tillåter i vissa särskilda fall personuppgiftsbehandling

[13] Datainspektionen kan i skrivande stund inte säga om misstanke om brott ska ingå bland personuppgifter om lagöverträdelser. Datainspektionen annonserar på sin hemsida att myndigheten avser att ge mer vägledning senare. www.datainspektionen.se.

utan samtycke. Ett ytterligare exempel är kamerabevakningslagen (2018:1200). Dataskyddsförordningen, liksom brottsdatalagen, ersätts eller kompletteras på ett stort antal verksamhetsområden av särskilda registerförfattningar, t.ex. polisdatalagen (2010:361)[14] inom den brottsbekämpande verksamheten och patientdatalagen (2008:355) inom hälso- och sjukvårdsverksamhet.

I 2 kap. 6 § RF används begreppet ”personlig integritet”. Begreppet har varit föremål för överväganden av flera statliga utredningar.[15] Det har också gjorts attitydundersökningar kring begreppet.[16] Man kan konstatera att dessa utredningar haft svårt att finna någon entydig och allmänt accepterad definition av begreppet.

Det finns alltså i nuläget inte någon definition av vad som avses med personlig integritet. Det beror på att begreppet rymmer en komplexitet som inte helt enkelt låter sig fångas i en enda bestämmelse och att ”personlig integritet” från tid till annan har olika innebörd. Svårigheterna att fastställa vad man menar med integritet sammanhänger också med att en rätt att bli lämnad i fred aldrig kan vara absolut i ett samhälle. Samhällets krav på insatser från den enskilde i fråga om t.ex. arbete och skatter kräver ibland inskränkningar i den privata sfären.[17]

I ett försök att ändå beskriva vad som kan anses vara kärnan i rätten till personlig integritet har regeringen i lagstiftningssammanhang uttalat att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång bör kunna avvisas.[18] Beskrivningen återkommer i regeringens direktiv till Integritetskommittén (dir: 2014:65 s. 2).

Sammanfattningsvis ger tidigare utredningar vid handen att med personlig integritet avses integritet i *ideell mening*, dvs. information om den enskildes personliga förhållanden. Skyddet för äganderätten, för den personliga friheten och rörelsefriheten eller för liv och hälsa faller utanför detta begrepp.

4.2 Registerförfattningar

Regeringen har i olika sammanhang uttalat att en specialreglering av behandling av personuppgifter under vissa förutsättningar innebär en bättre garanti för utformningen av integritetsskyddet än generella regleringar, t.ex. den tidigare personuppgiftslagen. Denna uppfattning har gett upphov till s.k. registerförfattningar, ”skräddarsydda” lagar eller förordningar som innehåller verksamhetsanpassade bestämmelser för en viss behandling av personuppgifter. Sådana registerförfattningar aktualiseras t.ex. i samband med myndighetsregister med ett stort antal registrerade

[14] Polisdatalagen ersätts den 1 januari 2019 av en ny lag om polisens behandling av personuppgifter inom brottsdatalagens område (prop. 2017/18:269).
[15] Se t.ex. SOU 1970:72 och 1980:8 (1966 års Integritetsskyddskommitté), SOU 1984:54 (Tvångsmedelskommittén), SOU 1992:84 (Kommittén om ideell skada), SOU 2002:18 (Integritetsutredningen), SOU 2004:20 (Kommittén om genetisk integritet) och SOU 2007:22 (2004 års Integritetsskyddskommitté).
[16] Se genomförd attitydundersökning av 2004 års Integritetskommitté i SOU 2007:22.
[17] SOU 1972:47 s. 56 f.
[18] Prop. 2009/10:80 s. 175, prop. 2005/06:173 s. 15.

personer och ett integritetskänsligt innehåll. Dessa registerförfattningar antingen kompletterade eller ersätta personuppgiftslagen.

Enligt dataskyddsförordningen får personuppgiftsbehandling inte endast stödja sig på förordningens bestämmelser när behandlingen sker på grund av

- en rättslig skyldighet,
- en arbetsuppgift av allmänt intresse eller
- myndighetsutövning.

Stöd måste finnas även i nationell rätt. Det innebär att flertalet registerförfattningar som beslutades under personuppgiftslagens giltighetstid alltjämt är i kraft. En väsentlig skillnad dock är att dessa specialförfattningar inte ersätter dataskyddsförordningen eller brottsdatalagen utan i stället kompletterar dem.

Behandling av personuppgifter av ”behöriga myndigheter” i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder omfattas av EU:s nya. Det har skett genom en ny brottsdatalag, som är en slags ramlag. Den ersätter inte t.ex. polisdatalagen och andra registerförfattningar inom det brottsutredande området, men gälla före dessa. Brottsdatalagen gäller också för behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet.

4.3 Särregler för brottsbekämpande verksamhet

I det följande berörs några registerförfattningar i orienterande syfte inom brottsdatadirektivets tillämpningsområde.

4.3.1 Polisen

Den huvudsakliga regleringen av polisens behandling av personuppgifter i den brottsbekämpande verksamheten finns i polisdatalagen (2010:361). Det finns dock även andra författningar som reglerar personuppgiftsbehandling i polisens brottsbekämpande verksamhet, framför allt lagstiftning som reglerar behandling i särskilda register. I 1 kap. 3 § polisdatalagen undantas från lagens tillämpningsområde behandling av personuppgifter enligt vapenlagen (1996:67), lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister och lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang.

Polisdatalagen gäller vid behandling av personuppgifter i brottsbekämpande verksamhet vid Polismyndigheten och Säkerhetspolisen och i Ekobrottsmyndighetens polisiära verksamhet, med undantag för behandling i de register som anges i 1 kap. 3 §. Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter. Lagen tillämpas enligt 1 kap. 6 § även i viss utsträckning på behandling av uppgifter om juridiska personer.

Några register regleras särskilt i 4 kap. polisdatalagen. Dessa är register över dna-profiler, dvs. dna-registret, utredningsregistret och spårregistret, fingeravtrycks- och signalementsregister, penningtvättsregister och det internationella registret. För dessa register finns särskilda bestämmelser om ändamål, gallring och direktåtkomst.

Polisdatalagen ersätts den 1 januari 2019 av en ny lag om polisens behandling av personuppgifter inom brottsdatalagens område.[19]

I annan verksamhet än den brottsbekämpande ska Polismyndigheten tillämpa dataskyddsförordningens bestämmelser, om det inte finns en specialreglering. Myndigheten tillämpar t.ex. utlänningsdatalagen (2016:27) i verksamhet som den bedriver enligt utlännings- och medborgarskapslagstiftningen, om det inte är fråga om brottsbekämpning.

I 2 kap. 15 § finns sekretessbrytande bestämmelser som anger i vilken utsträckning personuppgifter får lämnas ut till bl.a. Interpol och Europol, utländsk underrättelse- eller säkerhetstjänst och annan utländsk myndighet eller mellanfolklig organisation. Sekretessbrytande bestämmelser som gäller i förhållande till Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket finns i 2 kap. 16–18 §§ polisdatalagen.

I polisdatalagen finns hänvisningar till personuppgiftslagen. Enligt övergångsbestämmelserna till dataskyddslagen gäller den upphävda lagen (personuppgiftslagen) fortfarande i den utsträckning som det i en annan lag eller en förordning finns bestämmelser som innehåller hänvisningar till den lagen.

4.3.2 Nationellt forensiskt centrum

Nationellt forensiskt centrum, tidigare Statens kriminaltekniska laboratorium, är en avdelning inom Polismyndigheten. I 5 kap. polisdatalagen finns bestämmelser om personuppgiftsbehandling vid Polismyndigheten för forensiska ändamål. Där regleras framför allt ändamålen med sådan personuppgiftsbehandling som avviker från regleringen i övrigt i lagen, på grund av att avdelningen Nationellt forensiskt centrum har en särskild roll som expertmyndighet åt hela rättsväsendet.

Kapitlet innehåller även särskilda bestämmelser om bevarande och gallring. När det gäller behandling av känsliga personuppgifter, utlämnande av personuppgifter och uppgiftsskyldighet gäller i huvudsak samma bestämmelser som för Polismyndigheten.

4.3.3 Säkerhetspolisen

I 6 kap. polisdatalagen finns bestämmelser om behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet. Där regleras framför allt ändamålen för Säkerhetspolisens personuppgiftsbehandling, som delvis avviker från regleringen för Polismyndigheten. Det finns även särskilda bestämmelser om bevarande och gallring. När det gäller utlämnande av personuppgifter och

[19] Prop. 2017/18:269.

uppgiftsskyldighet gäller i huvudsak samma bestämmelser som för Polismyndigheten.

4.3.4 Övriga brottsbekämpande och brottsutredande myndigheter

I princip alla brottsutredande och brottsbekämpande myndigheter har en egen registerförfattning för behandling av personuppgifter för nu nämnda ändamål, såsom Tullverket, Kustbevakningen, Skatteverket och Åklagarmyndigheten.

4.3.5 Lagen om register över tillträdesförbud vid idrottsarrangemang

Lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang ger Polismyndigheten och idrottsorganisationer möjlighet att behandla personuppgifter för att på ett ändamålsenligt sätt kunna upprätthålla gällande beslut om tillträdesförbud vid idrottsarrangemang. Polismyndigheten får enligt 2 § med hjälp av automatiserad behandling föra ett tillträdesförbudsregister, som innehåller uppgifter om personer som har meddelats tillträdesförbud enligt lagen (2005:321) om tillträdesförbud vid idrottsarrangemang.

I förarbetena framhålls att Polismyndighetens personuppgiftsbehandling enligt lagen delvis är brottsbekämpande.[20]

4.4 Särregler för dömande verksamhet

För den dömande verksamheten gäller domstolsdatalagen (2015:728). Den är tillämplig på behandling av personuppgifter hos de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna. Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter.

Domstolsdatalagen är enligt 2 § – i motsats till polisdatalagen och Tullverkets och Skatteverkets motsvarande lagar – tillämplig i all rättskipande och rättsvårdande verksamhet vid de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna. Lagen gäller också när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran. Trots det mycket omfattande tillämpningsområdet regleras endast få frågor i domstolsdatalagen, vilket beror på den vittomfattande ändamålsregeln som medger behandling för handläggning av alla typer av mål och ärenden.

4.5 Register över ordningsbot och strafföreläggande

I förordningen (1997:902) om register över strafföreläggande regleras i 2 § Tullverkets rätt att föra register över utfärdade strafföreläggande, och i 3 § Polismyndighetens skyldighet att föra ett register över uppbörd i ärenden om strafföreläggande.

[20] Se Register över tillträdesförbud vid idrottsarrangemang, prop. 2013/14:254, s. 43.

Ett strafföreläggande register får enligt 6 § användas för handläggning av ärenden om strafföreläggande, för visst uppgiftslämnande och för framställning av statistik. I 9 § anges uttömmande vilka uppgifter ett strafföreläggande register får innehålla.

I förordningen (1997:903) om register över ordningsbot ges Polismyndigheten rätt att behandla personuppgifter i ett register över förelägganden av ordningsbot.

Registret används inte bara av Polismyndigheten utan även av Säkerhetspolisen, Tullverket och Kustbevakningen. All registrering av förelägganden av ordningsbot hanteras i registret.

Registret får enligt 2 § användas i ärenden om föreläggande av ordningsbot för handläggning, uppbörd och underrättelser till myndigheter samt för tillsyn, planering, uppföljning och framställning av statistik. I 5 § anges uttömmande vilka uppgifter registret får innehålla.

4.6 Regler om personuppgiftsbehandling hos andra aktörer än myndigheter

4.6.1 Uppgifter om brottsbekämpning, lagföring eller straffverkställighet

Det är inte bara myndigheter som behandlar uppgifter som rör brottsbekämpning, lagföring och straffverkställighet. Åtskilliga andra aktörer får i sin verksamhet i större eller mindre utsträckning tillgång till uppgifter om t.ex. domar i brottmål. I vilken utsträckning sådana uppgifter får behandlas regleras dels i dataskyddsförordningen, dels i andra författningar som kompletterar brottsdatalagen.

Som framhållits tidigare förbjuder dataskyddsförordningen andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, fällande domar i brottmål samt straffprocessuella tvångsmedel, t.ex. häktning, reseförbud eller beslag (art. 10). Det är i skrivande stund oklart om misstanke om brott utgör en personuppgift om lagöverträdelser.[21]

I 5 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning finns emellertid några undantag från förbudet. Personuppgifter om lagöverträdelser får behandlas av andra än myndigheter om behandlingen är nödvändig för att 1) rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, eller 2) en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras.

Enligt 6 § förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning får Datainspektionen meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla personuppgifter som avser lagöverträdelser. Sådana föreskrifter finns i Datainspektionens föreskrifter (DIFS 2018:2) om behandling av personuppgifter som rör lagöverträdelser.

Föreskrifterna innebär att personuppgifter om lagöverträdelser får behandlas bl.a. om behandlingen

- är nödvändig för att fullgöra en föreskrift på socialtjänstområdet,

[21] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/kansliga-personuppgifter/personuppgifter-som-ror-lagovertradelser/

- avser uppgift i anteckningar som förs i fristående skolors elevvårdande verksamhet eller i motsvarande verksamhet hos enskilda anordnare av högskoleutbildning,
- är nödvändig för att kontrollera att en jävssituation inte föreligger i advokatverksamhet eller annan juridisk verksamhet, eller
- avser personer i nyckelpositioner eller ledande ställning inom det egna bolaget eller koncernen och det är sakligt motiverat att behandla uppgifterna i särskilt inrättade rapporteringskanaler för att utreda om personen ifråga varit delaktig i allvarliga oegentligheter som rör bokföring, intern bokföringskontroll, revision, bekämpande av mutor, brottslighet inom bank- och finansväsen, eller andra allvarliga oegentligheter som rör organisationens vitala intressen eller enskildas liv och hälsa.

4.6.2 Offentliga försvarare och annat juridiskt biträde

I förundersökningar och brottmålsrättegångar biträds både den misstänkte och i vissa fall målsäganden av ett juridiskt biträde. Endast den som är advokat får enligt huvudregeln i 21 kap. 5 § rättegångsbalken utses till offentlig försvarare. Till målsägandebiträde får enligt 4 § lagen (1988:609) om målsägandebiträde jämförd med 26 § rättshjälpslagen (1996:1619) förordnas en advokat, en biträdande jurist eller någon annan som är lämplig för uppdraget. Motsvarande krav ställs på den som enligt 5 § lagen (1999:997) om särskild företrädare för barn får utses till särskild företrädare.

Den som fullgör uppgifter som offentlig försvarare, målsägandebiträde eller särskild företrädare för barn behandlar i stor utsträckning personuppgifter som härrör från förundersökningar, brottmålsrättegångar och straffverkställighet.

I 8 kap. rättegångsbalken finns bestämmelser om advokatväsendet. En advokat ska vara ledamot av Sveriges advokatsamfund, vars verksamhet delvis är av offentligrättslig natur genom den tillsyn som samfundets styrelse och disciplinnämnd enligt 8 kap. 6 och 7 §§ rättegångsbalken utövar över advokaterna.

Enligt 8 kap. 4 § rättegångsbalken ska en advokat i sin verksamhet redbart och nitiskt utföra de uppdrag som anförtrotts honom och iaktta god advokatsed.

Det finns inte några särregler för behandling av personuppgifter som utförs av någon av de kategorier som nämns i detta avsnitt. De tillämpar således dataskyddsförordningen.

4.6.3 Idrottsorganisationer

Som nämnts i avsnitts 4.3.5 får Polismyndigheten behandla personuppgifter i ett tillträdesförbudsregiser vid idrottsarrangemang. Även en idrottsorganisation får enligt 7 § lagen om register över tillträdesförbud vid idrottsarrangemang behandla personuppgifter från det tillträdesförbudsregister som Polismyndigheten för, om det behövs för att förebygga, förhindra eller upptäcka överträdelse av ett tillträdesförbud

vid ett idrottsarrangemang som organisationen anordnar. En sådan organisation har också enligt 9 § rätt att ta del av uppgifter i tillträdesförbudsregistret trots att det gäller sekretess för uppgifterna. Uppgifter ur tillträdesförbudsregistret får enligt 10 § lämnas ut till en idrottsorganisation på medium för automatiserad behandling.

4.7 Sekretess och tystnadsplikt

Bestämmelser om sekretess och tystnadsplikt i den offentliga förvaltningen finns i huvudsak i offentlighets- och sekretesslagen (2009:400; OSL). Bestämmelser om tystnadsplikt hos privata rättssubjekt regleras normalt i annan lagstiftning.

Sekretess definieras enligt OSL som ett *förbud att röja en uppgift*, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt (3 kap. 1 §). En bestämmelse om sekretess medför således både *tystnadsplikt* för de personer som har en skyldighet att följa bestämmelsen och *handlingssekretess* för de handlingar som omfattas av bestämmelsen.

När det gäller sekretessens styrka är det normala att den bestäms med hjälp av s.k. *skaderekvisit*. Man skiljer i detta avseende mellan rakt och omvänt skaderekvisit. Vid rakt skaderekvisit är utgångspunkten att uppgifterna är offentliga och att sekretess endast gäller om det kan antas att viss skada uppstår om uppgifterna lämnas ut. Vid omvänt skaderekvisitet är utgångspunkten den motsatta, dvs. att uppgifterna omfattas av sekretess. Vid omvänt skaderekvisit får uppgifterna således bara lämnas ut om det står klart att detta kan ske utan att viss skada uppstår. Sekretessen enligt en bestämmelse kan även vara absolut, vilket innebär att de uppgifter som omfattas av bestämmelsen ska hemlighållas utan någon skadeprövning.

Sekretess och tystnadsplikt kan aktualiseras inte bara när uppgifter begärs utlämnade av enskilda utan även när en myndighet självmant eller på begäran av en annan myndighet överväger att lämna ut uppgifter.

4.7.1 Samtycke häver sekretess

Det finns ett flertal undantag från sekretessen och tystnadsplikten. Undantagsbestämmelserna är spridda på flera lagar. De flesta undantagen är samlade i OSL. De berör olika slags fallsituationer där rättsordningen ansett att det är befogat att lämna ut uppgifter för olika ändamål utan en föregående menprövning.

Ett undantag från sekretessen finns i 12 kap. 2 § OSL. Enligt den bestämmelsen kan en enskild helt eller delvis häva sekretess som gäller till skydd för honom eller henne. Av denna bestämmelse framgår även att detta är huvudregeln, om inte annat anges i OSL. Någon menprövning i vanlig bemärkelse ska alltså inte göras i dessa lägen av utlämnande myndighet. Vad som måste kontrolleras emellertid är att uppgifterna lämnas ut till rätt mottagare. Lämnas de till fel mottagare kan fråga om sekretessbrott aktualiseras.

4.7.2 Sekretess i förhållande till den enskilde själv

Normalt råder inte sekretess eller tystnadsplikt enligt OSL i förhållande till den enskilde själv, men undantag finns, t.ex. uppgift i anmälan eller utsaga av en enskild om någons hälsotillstånd eller andra personliga förhållanden, i förhållande till den som anmälan eller utsagan avser (25 kap. 7 §) eller förundersökningssekretess (18 kap. 1 §).

Av den anledningen måste den som är ansvarig för en uppgift hos en myndighet alltid pröva en begäran om utlämnande i enlighet med OSL, trots att det är den enskilde själv som begär att få ut en handling eller uppgift om sig själv.

4.7.3 Sekretess inom brottsbekämpande och brottsutredande verksamheter

Gemensamt för myndigheterna i den s.k. rättskedjan är att sekretess i större eller mindre utsträckning gäller för flertalet av de uppgifter som utbyts mellan myndigheterna i brottmålsprocessen.

När en brottsutredning inleds gäller normalt sekretess enligt 18 kap. 1 § och 35 kap. 1 § OSL. Den förstnämnda sekretessen, utredningssekretess, minskar efterhand och brukar normalt upphöra senast i samband med att åtal väcks. Utredningssekretessen har ett rakt skaderekvisit, men kan inte efterges av den enskilde. Utredningssekretess kan således föreligga för uppgifter varhelst de finns och är av betydelse för en brottsutredning, t.ex. hos en vårdgivare.

Sekretess enligt 35 kap. 1 § OSL, som skyddar enskilds personliga och ekonomiska förhållanden bl.a. vid förundersökning, upphör också normalt om uppgiften lämnas till domstol, men kan kvarstå om domstol så förordnar (ursprungssekretess).

För att underlätta informationsutbytet mellan de brottsutredande myndigheterna inklusive åklagare i den utredande verksamheten finns bestämmelser om sekretessgenombrott. Dessa återfinns främst i 18 kap. och 35 kap. OSL.

Även den s.k. generalklausulen i OSL (10 kap. 27 §) är tillämplig i brottsutredningar och innebär att en sekretessbelagd uppgift får lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

4.7.4 Samverkan mot organiserad brottslighet

Polismyndigheten och flera andra myndigheter både inom rättskedjan och utanför den samverkar på olika sätt mot organiserad brottslighet. Regeringen har gett Polismyndigheten i uppdrag att tillsammans med dels myndigheter med brottsbekämpande uppgifter, dels några andra myndigheter att utveckla den myndighetsgemensamma satsningen mot organiserad brottslighet.

Lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet syftar till att förbättra samverkan och möjliggöra ett ökat informationsutbyte mellan myndigheter. Lagen föreskriver att vissa av regeringen utpekade myndigheter, trots sekretess, ska lämna ut uppgifter som en annan

myndighet behöver inom ramen för särskilt beslutad samverkan mellan myndigheter för att förebygga, förhindra eller upptäcka brottslig verksamhet som är av allvarlig eller omfattande karaktär och som bedrivs i organiserad form eller systematiskt av en grupp individer.

De myndigheter som regeringen pekar ut i förordningen (2016:775) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet är – förutom vissa myndigheter i rättskedjan – Arbetsförmedlingen, Försäkringskassan, Kronofogdemyndigheten och Migrationsverket. Kommuner och landsting nämns inte.

Skyldigheten att samverka medför inte att de myndigheter som är uppgiftsskyldiga och icke-brottsbekämpande blir behöriga myndigheter enligt brottsdatalagen (se avsnitt 8.3 angående gränsdragningsfrågor).

5 Ny dataskyddsförordning

Från och med den 25 maj 2018 gäller EU:s allmänna dataskyddsförordning (dataskyddsförordningen). Dataskyddsförordningen har företräde framför nationell rätt, vilket innebär att om nationell lagstiftning inte överensstämmer med förordningen, ska förordningens bestämmelser tillämpas. Dataskyddsförordningen lämnar dock visst utrymme för, och påbjuder även i vissa fall, nationella regler. Det kommer därför fortsatt finnas nationella dataskyddsregler, s.k. registerförfattningar.

5.1 Ändringar i stort

Dataskyddsförordningen baseras till stor del på dataskyddsdirektivets struktur och innehåll, men innebär även en rad förändringar. Några av dessa förtjänar att nämnas särskilt.

5.1.1 Grundläggande principer

De grundläggande kraven i 9 § personuppgiftslagen (1998:204; PUL) har blivit grundläggande dataskyddsprinciper för behandling av personuppgifter och dataskydd (art. 5). Dessutom har nya principer tillkommit. En sådan är principen om öppenhet (transparens) gentemot den registrerade som kommer till uttryck i skyldigheten för personuppgiftsansvariga att informera registrerade om personuppgiftsbehandlingen (art. 13 och 14). Kravet på öppenhet (transparens) har stärkts betydligt.

Integritet och konfidentialitet har lyfts in i de grundläggande principerna. Ett nytt krav har tillkommit som anger att den personuppgiftsansvarige inte bara ansvarar för att de grundläggande principerna följs utan också ska kunna ”visa” att de efterlevs, s.k. ansvarsskyldighet (art. 5.2).

5.1.2 Information till den registrerade

Den information som ska tillhandahållas den registrerade har *preciserats och utvidgats* och det anges uttryckligen att den personuppgiftsansvarige ska tillhandahålla informationen i en begriplig och lättillgänglig form. Det ska enligt förordningen aldrig komma som en överraskning för en registrerad att någon hanterar dennes personuppgifter och för vilka ändamål. Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av dessa personuppgifter är

lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används (skäl 39). Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, bör allmän information ges (skäl 61).

5.1.3 Registrerades rättigheter

Den registrerades rättigheter har förstärkts i syfte att ge den registrerade ökad kontroll över sina personuppgifter. Det finns åtta rättigheter. Flera rättigheter är nya. Som exempel kan nämnas en förstärkning av rätten att få åtkomst till sina personuppgifter i syfte att föra över dem till en annan leverantör av elektroniska tjänster, s.k. dataportabilitet. Vidare har en tydligare rätt till radering (”rätt att bli bortglömd”) införts.

5.1.4 Lagliga grunder för personuppgiftsbehandling

De rättsliga grunderna för personuppgiftsbehandling är i stort sett desamma som i det nuvarande dataskyddsdirektivet. I dataskyddsförordningen räknas dessa rättsliga grunder upp i artikel 6.1.

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål
b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn (*intresseavvägning*).

5.1.5 Tydligare krav på samtycke

En rättslig grund för personuppgiftsbehandling är samtycke (se föregående underrubrik). Dataskyddsförordningen ställer tydligare krav på ett samtycke än PUL. Bl.a. ska den personuppgiftsansvarige kunna ”visa” att man har fått ett samtycke från den registrerade för att behandla dennes personuppgifter. Samtycken ska vara klara och tydliga - att dölja samtycken i långa snåriga användaravtal kommer inte att duga längre.

Används personuppgifter för ett nytt ändamål ska enligt dataskyddsförordningen den personuppgiftsansvarige inhämta ett samtycke även för den behandlingen. Det ska vara lika lätt att återkalla som att ge sitt samtycke (art. 7.3). Det innebär i praktiken att en personuppgiftsansvarig, efter att samtycket har återkallats, inte får genomföra någon ny behandling av personuppgifter som kräver samtycke och, om individen begär det och annan laglig grund för behandlingen saknas, måste ta bort personuppgifterna från informationssystem.

Det införs ett krav på att i vissa fall inhämta samtycke från vårdnadshavare eller godkännande av barnets samtycke när informationssamhällets tjänster erbjuds direkt till ett barn. Enligt dataslyddslagen krävs vårdnadshavares samtycke när barnet är 11 år eller yngre. Barns särställning och särskilda utsatthet poängteras på flera ställen i förordningen.

5.1.6 Intresseavvägning

Tidigare, enligt PUL, fick myndigheter behandla personuppgifter efter en intresseavvägning. Det innebär att om det inte finns samtycke till personuppgiftsbehandlingen eller någon annan laglig grund, tillät PUL att myndigheten fick behandla personuppgifter för ett berättigat intresse om myndighetens intresse av behandlingen vägde tyngre än den registrerades intresse av skydd mot kränkningar av den personliga integriteten. PUL:s regel om intresseavvägning gäller dock inte längre för myndigheter enligt dataskyddsförordningen, ”när de fullgör sina uppgifter”. Myndigheter kan alltså numera inte längre åberopa ”intresseavvägning” för personuppgiftsbehandling.

5.1.7 Personuppgiftsansvaret m.m.

Genom förordningen har det införts en skyldighet för den personuppgiftsansvarige att anmäla till tillsynsmyndigheten om det inträffar en så kallad personuppgiftsincident, dvs. en säkerhetsincident som oavsiktligt påverkar behandlingen av personuppgifter. Även den registrerade ska informeras om incidenten om den sannolikt leder till en hög risk för enskildas rättigheter och friheter. Även personuppgiftsbiträden ska anmäla personuppgiftsincidenter till den personuppgiftsansvarige.

Dataskyddsförordningen ställer också krav på den personuppgiftsansvarige att genomföra konsekvensanalyser om en viss behandling sannolikt kommer att leda till hög risk för enskildas rättigheter eller skyldigheter. Den allmänna anmälningsskyldigheten till tillsynsmyndigheten är borttagen. Vidare innehåller dataskyddsförordningen tydligare regler om säkerheten för personuppgifter. Ett krav på inbyggt dataskydd och dataskydd som standard har införts.

5.1.8 Sanktionsavgifter m.m.

Genom förordningen har det införts ett nytt gemensamt system med administrativa sanktionsavgifter som ska tas ut vid vissa typer av överträdelser av förordningen. Personuppgiftsbiträden får ett begränsat skadeståndsansvar (art. 82). Även på andra sätt innebär förordningen ett ökat fokus på en enhetlig tillämpning av dataskyddsreglerna inom EU, t.ex. genom åtgärder som godkännande av uppförandekoder och certifiering. Det har även införts en skyldighet för de nationella tillsynsmyndigheterna att samarbeta med varandra. Det har också införts en ny princip om en enda kontaktpunkt, som ska underlätta för sådana personuppgiftsansvariga som är verksamma i flera medlemsstater genom att de endast ska behöva vara i kontakt med en av de behöriga tillsynsmyndigheterna. Ett nytt unionsorgan, Europeiska dataskyddsstyrelsen, har ersatt Artikel 29-arbetsgruppen och som får långtgående befogenheter att uttala sig om tolkningen av förordningen även i enskilda fall.

5.2 Undantag från bestämmelserna

Dataskyddsförordningen gäller inte för personuppgifter som behandlas av:

- Privatpersoner som behandlar personuppgifter i verksamhet av rent privat natur eller för sitt eget och familjens bruk.
- Polisen och andra myndigheter, om uppgifterna ingår i brottsbekämpande verksamhet.
- Försvaret samt säkerhets- och underrättelsetjänster.
- Myndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut allmänna handlingar (offentlighetsprincipen)

Därutöver kan medlemsstaterna införa särskilda undantag från stora delar av dataskyddsförordningens bestämmelser om det är nödvändigt för att förena rätten till integritet med yttrande- och informationsfriheten för till exempel:

- Massmedier med utgivningsbevis när det gäller journalistiskt arbete och publicering.
- Arkiv, museer och bibliotek.
- Litterärt och konstnärligt arbete.

Försvarsmakten har emellertid inte undantagits förordningens bestämmelser. Däremot ska enligt dataskyddslagen bestämmelserna i dataskyddsförordningen inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Enligt dataskyddslagen ska artiklarna 5-30 och 35-50 i dataskyddsförordning samt 2-5 kap. i lagen inte heller tillämpas vid behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

6 Brottsdatadirektivet

I det följande lämnas en orientering om brottsdatadirektivet. Sverige genomförde direktivet genom en ny brottsdatalag som trädde i kraft den 1 augusti 2018 (se avsnitt 7).

6.1 Innehållet i direktivet

Enligt artikel 1 innehåller direktivet bestämmelser om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter i syfte att *förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot och förebygga och förhindra hot mot den allmänna säkerheten.*

Syftet med direktivet är att dels skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, dels säkerställa att, när det krävs utbyte av personuppgifter inom unionen mellan behöriga myndigheter, detta utbyte varken begränsas eller förbjuds av hänsyn till skyddet för fysiska personer mot behandling av personuppgifter. Det slås också fast att direktivet inte hindrar att medlemsstaterna föreskriver strängare skyddsåtgärder när det gäller registrerades rättigheter och friheter.

Artikel 2 anger direktivets tillämpningsområde. Direktivet ska tillämpas på behandling av personuppgifter som utförs av ”*behöriga myndigheter*” för de ändamål som anges i artikel 1.1. Med ”behörig myndighet” avses enligt direktivet

a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten, eller

b) annat organ eller annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten,

Direktivet ska tillämpas dels på helt eller delvis automatiserad behandling av personuppgifter, dels på annan behandling av personuppgifter som ingår i eller kommer att ingå i register. Däremot ska direktivet inte tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller på personuppgiftsbehandling som utförs av unionens institutioner eller andra organ.

6.2 Principer – artiklarna 4 – 11

I artikel 4 anges grundläggande principer för behandling av personuppgifter. De motsvarar med något undantag i stort de grundläggande principerna i dataskyddsförordningen. Personuppgifter ska

- behandlas på ett lagligt och korrekt sätt,
- samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,
- vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,
- vara korrekta och, om nödvändigt, uppdaterade,
- inte möjliggöra identifiering av den registrerade under längre tid än nödvändigt, och
- behandlas på ett sätt som säkerställer säkerheten för uppgifterna.

Behandling för något annat ändamål som anges i artikel 1.1 än det för vilket uppgifterna samlades in är tillåten om den personuppgiftsansvarige har rätt att behandla personuppgifter för ett sådant ändamål och behandlingen är nödvändig och står i proportion till det nya ändamålet. Behandlingen kan inkludera arkivändamål som är av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som anges i artikel 1.1, om det finns lämpliga skyddsåtgärder.

Enligt artikel 5 ska lämpliga tidsgränser föreskrivas för när personuppgifter ska raderas eller för regelbunden översyn av behovet av att lagra sådana uppgifter. Det ska finnas regler för att säkerställa att tidsgränserna hålls.

Enligt artikel 6 ska den personuppgiftsansvarige så långt möjligt göra åtskillnad mellan personuppgifter som rör olika kategorier av registrerade, som misstänkta, dömda, brottsoffer och andra som berörs av brott, exempelvis personer som kan komma att kallas som vittnen.

I artikel 7 föreskrivs att åtskillnad så långt möjligt ska göras mellan personuppgifter som grundar sig på *fakta* och uppgifter som grundar sig på *personliga bedömningar*. Behöriga myndigheter ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Om felaktiga personuppgifter har överförts eller personuppgifter överförts olagligen ska mottagaren omedelbart underrättas om det. I sådana fall ska personuppgifterna rättas eller raderas eller behandlingen av dem begränsas.

Enligt artikel 8 är behandling laglig endast om och i den utsträckning behandlingen är *nödvändig* för att behöriga myndigheter ska kunna utföra sådana uppgifter som anges i artikel 1.1 *och som grundas på unionsrätt eller nationell rätt*. Den nationella rätten ska åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och ändamålet med behandlingen.

I artikel 9 föreskrivs att personuppgifter som samlats in för något av de i direktivet angivna ändamålen inte får behandlas för något annat ändamål om inte sådan behandling är tillåten enligt unionsrätten eller nationell rätt. När personuppgifter behandlas för andra ändamål än dem som anges i artikel 1.1 ska dataskyddsförordningen tillämpas, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten. *Om de behöriga myndigheterna har andra uppgifter än dem som anges i artikel 1.1, ska dataskyddsförordningen tillämpas på behandling för sådana ändamål.* Det gäller även behandling för

arkivändamål som är av allmänt intresse eller för statistiska, historiska eller vetenskapliga ändamål. I artikeln anges också vad som gäller för överföring av uppgifter för behandling för andra ändamål.

Artikel 10 reglerar behandling av det som brukar kallas *känsliga personuppgifter*. Med det avses uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Regleringen omfattar även behandling av genetiska uppgifter, biometriska uppgifter i identifieringssyfte eller uppgifter om hälsa, sexualliv eller sexuell läggning.

Behandling av sådana uppgifter är bara tillåten om den är absolut nödvändig, det finns tillräckliga skyddsåtgärder och behandlingen är tillåten enligt unionsrätt eller nationell rätt för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person eller om det är fråga om uppgifter som den registrerade själv har offentliggjort.

I artikel 11 förbjuds att beslut, som har negativa rättsverkningar eller i betydande grad påverkar den registrerade, fattas om de enbart grundas på automatiserad behandling, såvida inte de är tillåtna enligt unionsrätten eller nationell rätt och det finns lämpliga skyddsåtgärder. Profilering som leder till diskriminering på grundval av känsliga personuppgifter ska förbjudas.

6.3 Den registrerades rättigheter – artiklarna 12 – 18

Enligt artikel 12 ska den personuppgiftsansvarige utan kostnad lämna den registrerade information om hans eller hennes rättigheter. Informationen ska vara koncis, lättillgänglig och språkligt lättfattlig. Den personuppgiftsansvarige ska utan onödigt dröjsmål skriftligen besvara en begäran från den registrerade om information om hur hans eller hennes personuppgifter behandlas. Om en registrerads begäran är uppenbart ogrundad eller orimlig får den personuppgiftsansvarige antingen ta ut en avgift eller vägra tillmötesgå begäran.

I artikel 13 anges vilken information som alltid måste göras tillgänglig för den registrerade. Det är den personuppgiftsansvariges identitet och kontaktuppgifter, dataskyddsombudets kontaktuppgifter, ändamålen med den avsedda behandlingen, rätten att klaga till en tillsynsmyndighet och dess kontaktuppgifter och rätten att begära att få del av personuppgifter, rättelse, radering eller begränsning av behandlingen. Därutöver ska den personuppgiftsansvarige i specifika fall lämna viss annan information för att göra det möjligt för den registrerade att utöva sina rättigheter.

Artikel 14 behandlar den registrerades rätt till tillgång till personuppgifter. Om inte annat sägs i artikel 15 ska den registrerade ha rätt att av den personuppgiftsansvarige få bekräftelse på om personuppgifter som rör honom eller henne behandlas och, om så är fallet, få tillgång till personuppgifterna och viss information:

Enligt artikel 15 får medlemsstaterna genom lagstiftning, så länge åtgärden är nödvändig och proportionell, helt eller delvis begränsa den registrerades rätt till

tillgång till personuppgifter och information i syfte att undvika att förundersökningar och andra utredningar eller förfaranden, brottsbekämpande åtgärder, lagföring eller verkställighet av straffrättsliga påföljder försvåras eller i syfte att skydda allmän säkerhet, nationell säkerhet eller andra personers rättigheter och friheter.

Artikel 16 behandlar rätten till rättelse eller radering av personuppgifter eller begränsning av behandlingen och vilka skyldigheter den personuppgiftsansvarige har i sådana frågor.

Enligt artikel 17 ska den registrerades rättigheter även kunna utövas genom den behöriga tillsynsmyndigheten om tillgången till information har begränsats.

I artikel 18 öppnas möjlighet att föreskriva att rätten till information, tillgång till uppgifter, rättelse, radering och begränsning av behandling ska utövas enligt nationell rätt om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredning och straffrättsliga förfaranden.

Av skäl 107 framgår att direktivet inte hindrar att det i nationell straffprocesslagstiftning finns bestämmelser om den registrerades rätt till information, tillgång till och rättelse eller radering av personuppgifter och begränsning av behandling i samband med straffrättsliga förfaranden och begränsningar i dessa rättigheter.

6.4 Personuppgiftsansvarig och personuppgiftsbiträde – artiklarna 19 – 28

Den personuppgiftsansvarige ska enligt artikel 19 vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter utförs i enlighet med direktivet.

Artikel 20 behandlar inbyggt dataskydd och dataskydd som standard.

Artikel 21 öppnar en möjlighet att låta två eller flera personuppgiftsansvariga ha gemensamt personuppgiftsansvar för ett register.

I artikel 22 regleras vilka krav som ställs när en personuppgiftsansvarig anlitar ett personuppgiftsbiträde.

Artikel 24 innehåller detaljerade regler om personuppgiftsansvarigas skyldighet att föra register över olika typer av behandlingar. I artikel 25 ställs krav på att det ska finnas loggar över olika typer av behandling i automatiserade behandlingssystem. Registren och loggarna ska på begäran göras tillgängliga för tillsynsmyndigheten.

Enligt artikel 26 ska personuppgiftsansvariga och personuppgiftsbiträden på begäran samarbeta med tillsynsmyndigheten.

I artikel 27 ställs krav på att den personuppgiftsansvarige gör en dataskyddskonsekvensbedömning för skyddet av personuppgifter när det gäller en ny typ av behandling som sannolikt leder till hög risk för fysiska personers rättigheter och friheter.

Artikel 28 ställer krav på att den personuppgiftsansvarige under vissa förutsättningar ska samråda med tillsynsmyndigheten innan nya register inrättas.

6.5 Säkerhet för personuppgifter – artiklarna 29 – 31

Artikel 29 innehåller krav på säkerhet i samband med behandlingen av personuppgifter. Den personuppgiftsansvarige och personuppgiftsbiträdet ska – med beaktande av bl.a. kostnaderna och behandlingens art, omfattning och ändamål – vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa lämplig säkerhetsnivå. Säkerheten ska omfatta åtkomstskydd för utrustning, kontroll av datamedier, lagringskontroll, användarkontroll, åtkomstkontroll, kommunikationskontroll, indatakontroll, transportkontroll, återställande, driftsäkerhet och dataintegritet.

I artikel 30 regleras den personuppgiftsansvariges skyldigheter om det inträffar en personuppgiftsincident. En sådan ska anmälas till tillsynsmyndigheten utan dröjsmål och enligt huvudregeln senast 72 timmar efter att den personuppgiftsansvarige har fått kännedom om incidenten. I artikeln anges också vad en sådan anmälan ska innehålla och vilken dokumentation om incidenten som krävs.

Artikel 31 innehåller regler om information till den registrerade om en personuppgiftsincident och i vilka fall det inte krävs någon sådan information.

6.6 Dataskyddsombud – artiklarna 32 – 34

Enligt artikel 32 ska den personuppgiftsansvarige utnämna ett dataskyddsombud. Undantag får göras för domstolars och andra oberoende rättsliga myndigheters dömande verksamhet. Flera myndigheter får ha samma dataskyddsombud. Ombudets kontaktuppgifter ska dels offentliggöras, dels meddelas till tillsynsmyndigheten. Artiklarna 33 och 34 berör ombudets uppgifter och ställning.

6.7 Överföring av personuppgifter till tredjeländer eller internationella organisationer – artiklarna 35 – 40

I artikel 35 anges allmänna principer för överföring av personuppgifter till tredjeland och internationella organisationer. Där föreskrivs bl.a. att överföringen ska vara nödvändig för något av de ändamål som anges i artikel 1.1 och att den ska riktas till en personuppgiftsansvarig i ett tredjeland eller en internationell organisation som är behörig för sådana ändamål. Om uppgifterna kommer från en annan medlemsstat ska den enligt huvudregeln ge förhandstill-stånd till överföringen.

Artikel 36 reglerar överföring till mottagare i tredjeland eller internationella organisationer som enligt kommissionens beslut har en adekvat skyddsnivå. Sådana överföringar kräver inte särskilt tillstånd.

Även om det inte finns något beslut om en adekvat skyddsnivå får, enligt artikel 37, uppgifter överföras till mottagare i ett tredjeland eller en internationell organisation om lämpliga skyddsåtgärder kan säkerställas i ett enskilt fall.

I artikel 38 görs också undantag för överföring i särskilda situationer, bl.a. för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en medlemsstat eller ett tredjeland.

Artikel 39 reglerar överföring direkt till vissa mottagare som inte är behöriga myndigheter.

Kommissionen och medlemsstaterna åläggs i artikel 40 att bl.a. utveckla rutiner för det internationella samarbetet för att underlätta en effektiv tillämpning av lagstiftningen om skydd för personupp-gifter och att också erbjuda bistånd till tredjeland och internationella organisationer i det syftet.

6.8 Rättsmedel, ansvar och sanktioner – artiklarna 52 – 57

Artikel 52 reglerar rätten för registrerade att lämna in klagomål över personuppgiftsbehandling till en tillsynsmyndighet. Har klagomålet lämnats till fel myndighet ska den utan dröjsmål överlämna klagomålet till rätt myndighet. Den registrerade ska underrättas om handläggningen av klagomålet och vad det resulterar i.

Rätten till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde regleras i artikel 54.

Den som lidit skada till följd av olaglig behandling av person-uppgifter eller någon annan åtgärd som står i strid med de bestämmelser som genomför direktivet ska enligt artikel 56 ha rätt till ersättning från den personuppgiftsansvarige eller annan myndighet som är behörig enligt nationell rätt.

Artikel 57 ställer krav på att det finns sanktioner för överträdelser av de bestämmelser som genomför direktivet. Sanktionerna ska vara effektiva, proportionella och avskräckande.

7 Dataskyddslagen och brottsdatalagen

7.1 Inledning

Som framhållits har den Europeiska unionen enats om en genomgripande dataskyddsreform som genomfördes under våren 2018. Reformen omfattar dels en allmän dataskyddsförordning, dels ett dataskyddsdirektiv som behandlar dataskyddet vid bl.a. brottsbekämpning, lagföring och straffverkställighet (brottsdatadirektivet). En konsekvens av reformen är att personuppgiftslagen har upphävts och att regeringen har sett över all lagstiftning om personuppgiftsbehandling och anpassat den till de nya EU-rättsliga dataskyddsbestämmelserna.

Översynen har bl.a. resulterat i dels en ny lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen), dels en ny brottsdatalag (2018:1177). I det följande lämnas en kort orientering om dessa registerförfattningar.

7.2 Brottsdatalagen

Den 17 mars 2016 uppdrog regeringen åt en särskild utredare att föreslå hur brottsdatadirektivet ska genomföras i svensk lagstiftning (dir. 2016:21). Utredningen, som tog sig namnet Brottsdatautredningen (SOU 2017:29), föreslog att brottsdatadirektivet i huvudsak genomförs genom en ny lag, brottsdatalagen (2018:1177).

Brottsdatalagen trädde i kraft den 1 augusti 2018.[22] Syftet med lagen är både att skydda fysiska personers grundläggande fri- och rättigheter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt (1 kap. 1 §). Vad som avses med en behörig myndighet redovisas nedan.

Brottsdatalagen är subsidiär, dvs. om en annan lag eller en förordning innehåller någon bestämmelse som avviker från lagen, ska den bestämmelsen tillämpas (1 kap. 5 §). Denna undantagsregel beror på att flertalet myndigheter som bedriver verksamhet inom lagens tillämpningsområde ska beakta särskilda registerförfattningar som reglerar personuppgiftsbehandlingen, t.ex. polisdatalagen och åklagardatalagen.

Lagen ska tillämpas bara av myndigheter som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder vid behandling av personuppgifter. Lagen ska

[22] Prop. 2017/18:232.

också gälla för personuppgiftsbehandling vid upprätthållande av allmän ordning och säkerhet. De myndigheter som har sådana arbetsuppgifter betecknas ”behöriga myndigheter” i lagen (1 kap. 2 §). Lagen ska dock även tillämpas av andra aktörer som har fått i uppgift att utöva myndighet för något av de nämnda syftena.

De behöriga myndigheternas behandling av personuppgifter kommer dock bara att styras av lagen när de behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Dataskyddsförordningen kommer att bli tillämplig i övrigt, t.ex. när Polismyndigheten behandlar personuppgifter i tillståndsärenden eller när en allmän domstol handlägger ett tvistemål. Det som blir avgörande för om lagen är tillämplig är dels om det är en ”behörig myndighet” som behandlar personuppgifterna, dels syftet med behandlingen.

Lagen har kompletterats med en brottsdataförordning (2018:1202), som genomför vissa detaljbestämmelser i direktivet.

7.3 Dataskyddslagen

Regeringen beslutade den 25 februari 2016 att tillkalla en särskild utredare med uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som den nya dataskyddsförordningen gav anledning till. Utredningen, som tog namnet Dataskyddsutredningen (SOU 2017:39), presenterade en ny dataskyddslag.

Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) trädde i kraft den 25 maj 2018.[23] . Lagen kompletterar dataskyddsförordningen och tar inte över förordningen på något sätt. Sektorsspecifika registerförfattningar ska dock ha företräde framför dataskyddslagen.

Enligt dataskyddsförordningen måste en rättslig skyldighet, myndighetsutövning eller arbetsuppgift av allmänt intresse vara fastställd i enlighet med nationell rätt eller unionsrätt för att kunna utgöra rättslig grund för behandling av personuppgifter. I dataskyddslagen finns bestämmelser som förtydligar hur dessa företeelser fastställs i enlighet med svensk rätt.

En rättslig förpliktelse är enligt svensk rätt fastställd om den gäller enligt lag eller annan författning eller följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Myndighetsutövning fastställs i svensk rätt genom lag eller annan författning. Uppgifter av allmänt intresse är fastställda i enlighet med svensk rätt om de följer av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Enligt förordningen ska ett barn ha fyllt 16 år för att självt kunna samtycka till behandling av personuppgifter vid erbjudandet av informationssamhällets tjänster, t.ex. sociala medier, söktjänster och s.k. appar för smarta enheter. I dataskyddslagen

[23] Prop. 2017/18:105.

har åldern sänkts till 13 år. För barn yngre än så krävs att samtycket lämnas av vårdnadshavaren eller att barnets samtycke godkänns av denne.

Enligt dataskyddsförordningen gäller som huvudregel ett förbud mot behandling av *känsliga personuppgifter*. Behandling av sådana personuppgifter får ske bara om det finns stöd i någon av förordningens undantagsbestämmelser. Vissa undantag från förbudet följer direkt av förordningen, medan andra förutsätter stöd även i nationell rätt. I dataskyddslagen finns ett sådant stöd när det gäller nödvändig behandling av personuppgifter på arbetsrättens område, inom hälso- och sjukvård, i social omsorg, i arkivverksamhet och i statistisk verksamhet. Stödet för behandlingen ska vara förenat med vissa restriktioner.

Myndigheter har dock fått vidgade möjligheter att få behandla känsliga personuppgifter. Behandling får ske i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ett ärende, om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, eller i enstaka fall, om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Myndigheter får med stöd av dataskyddslagen behandla personuppgifter som rör *fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel*. För att andra än myndigheter ska få behandla sådana uppgifter måste det finnas uttryckligt stöd i lag eller förordning eller i föreskrifter eller förvaltningsbeslut från Datainspektionen. Lagen innehåller ett sådant stöd när det gäller uppgifter som behandlas för arkivändamål av allmänt intresse, förutsatt att behandlingen sker som en följd av de skyldigheter att bevara och vårda handlingar som anges i arkivlagstiftningen och andra föreskrifter.

Vissa viktiga undantag från enskildas rättigheter regleras direkt i förordningen. Dataskyddslagen innehåller ytterligare undantag. Rätten till information och s.k. registerutdrag ska inte gälla för uppgifter som omfattas av sekretess. Rätten till registerutdrag ska som huvudregel inte heller gälla personuppgifter som finns i löpande text som utgör utkast eller minnesanteckning.

I likhet med vad som gällde enligt den tidigare personuppgiftslagen ska vissa beslut som en myndighet fattar i egenskap av personuppgiftsansvarig kunna överklagas till allmän förvaltningsdomstol. Det gäller sådana beslut som myndigheten fattar med anledning av att den registrerade utövar sina rättigheter enligt dataskyddsförordningen. Det kan t.ex. röra sig om avslagsbeslut på begäran om att den registrerade ska få tillgång till sina personuppgifter, att uppgifter ska rättas eller raderas eller att en behandling ska begränsas.

Den registrerade har enligt dataskyddsförordningen rätt till ersättning från den personuppgiftsansvarige eller ett personuppgiftsbiträde om skada har uppstått på grund av överträdelser av förordningen. Av dataskyddslagen framgår att denna rätt till skadestånd även gäller vid överträdelser av bestämmelser i dataskyddslagen och andra författningar som kompletterar förordningen.

Genom dataskyddsförordningen införs en skyldighet för myndigheter och vissa företag att utse ett dataskyddsombud. Ombudet ska vara bundet av sekretess enligt unionsrätten eller den nationella rätten.

8 Bedömning

Den övergripande frågan som ska besvaras i denna laglighetsprövning är i vilken utsträckning personuppgifter behandlas, och får lagligen behandlas i Embrace, och av vem (laglighetsprövning).

I det följande övervägs frågeställningarna som återfinns i kapitel 3.

8.1 Behandlar Embrace personuppgifter?

Bedömning: Embrace registrerar inte enskilda individer utan enbart brottsrelaterade och andra otrygghetsskapande händelser. Embrace är inte designat för att registrera individuppgifter. Tekniska och administrativa mekanismer finns inbyggda i tjänsten för att förhindra sådan registrering.

För att kunna analysera brottsrelaterade och andra otrygghetsskapande händelser samt följa upp insatser som ska motverka sådana händelser krävs emellertid registrering av exakta platsuppgifter, t.ex. gatu- och adressuppgifter. Sådana uppgifter kan indirekt hänföras till en fysisk levande person, t.ex. en familj vars villa har utsatts för skadegörelse på fasaden.

Övervägande skäl talar för att Embrace i de fall tjänsten innehåller uppgifter om gatu- och fastighetsadresser där en eller flera fysiska personer har sitt hushåll behandlar personuppgifter i dataskyddsförordningens och brottsdatalagens mening, trots att det inte är det huvudsakliga syftet med tjänsten att registrera enskilda individer.

Registrering av uppgifter/händelser som inträffar på allmänna platser, t.ex. torg, parker eller köpcentra utgör däremot inte personuppgifter eftersom dessa adressuppgifter inte eller sällan kan hänföras till enskilda individer på något sätt.

8.1.1 Gällande rätt och praxis

En av frågeställningarna som ska besvaras är om molntjänsten Embrace hanterar personuppgifter.

Begreppet ”personuppgifter” är hämtat från dataskyddsförordningen. Med personuppgift avses varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller

sociala identitet (art. 4.1). Av den exemplifiering som framgår av definitionen har en kodifiering skett av praxis kring nätverksadresser eller motsvarande såsom utgörande personuppgifter. Någon förändring av begreppet personuppgifter synes dock inte ha skett. Därför får den praxis som utvecklats kring begreppet personuppgifter i den tidigare personuppgiftslagen anses relevant.

Brottsdatalagen har en likalydande, men kortare definition på personuppgifter: Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet (1 kap. 6 §). Brottsdatalagens definition motsvarar i huvudsak definitionen på personuppgifter som fanns i den tidigare personuppgiftslagen. Båda definitionerna i förordningen respektive brottsdatalagen får anses ha samma innebörd, trots att definitionerna skiljer sig något åt.

Det uppställs således inga kvalitetskrav på informationen om en person för att förordningen eller brottsdatalagen ska bli tillämpliga, t.ex. att det ska vara fråga om vissa särskilt privata eller känsliga uppgifter. Det är tillräckligt att det är fråga om information som kan hänföras till en viss identifierbar individ.

Uppgifter om juridiska personer omfattas inte i sig av definitionen, även om den juridiska personen skulle råka ägas av en eller ett fåtal fysiska personer eller ha en benämning (firma) som innefattar ett personnamn. Däremot omfattas uppgifter om en enskild firma, eftersom innehavaren av en sådan firma alltid är en enda fysisk person. Justitiekanslern har t.ex. ansett att uppgifter om en namngiven kennel, som drivs av en person, utgör personuppgifter (beslut 2008-05-28, dnr 7379-06-42).

Svea hovrätt har ansett att registreringsnumret för en enskild firma, vilket innehåller personnumret för den som står bakom firman, utgör en personuppgift, ett personnummer (dom 2004-08-31 i mål nr B 4151–04).

För att avgöra om en person är identifierbar ska alla hjälpmedel beaktas som i syfte att identifiera vederbörande rimligen kan komma att användas av antingen den som är ansvarig för behandlingen (den personuppgiftsansvarige), eller av någon annan person. Begreppet personuppgift omfattar vidare all information om individer, oavsett deras ställning eller kapacitet.

Som exempel på personuppgifter kan nämnas personnummer, registreringsnummer för fordon och kundnummer.

Uppgifter om födelsetid jämte postnummer till hemadressen har ansetts utgöra personuppgifter, se Kammarrätten i Stockholms dom 2001-06-19 i mål nr 1138–2001. Däremot anses inte en isolerad uppgift om födelsedatum utgöra en personuppgift, ens om uppgiften hämtas manuellt från legitimationshandlingar, se Länsrätten i Stockholms läns dom 2006-06-09 i mål nr 7055–2005.

Redan namnet på en person är givetvis en personuppgift (se t.ex. Datainspektionens ärende dnr 1062–99, som gällde Borlänge kommuns publicering på internet av 47 772 namn på kommuninvånare).

Datainspektionen har i ett flertal ärenden gjort bedömningen att elektroniska passagesystem i bostadsrätts- och hyreshus, där lägenhetsnummer kopplas till en eller flera personer, innebär en behandling av personuppgifter i PUL:s mening (se

bl.a. beslut 2006-02-27, dnr 130–2006). Lägenhetsnummer betraktas således som en personuppgift.

Datainspektionen har vidare i ett samrådsyttrande tagit ställning till om hur personuppgifter får användas vid utveckling av ny teknik för bildinformation i geografiska informationssystem (GIS) (samrådsyttrande 2008-04-09, dnr 1070–2007). Linköpings kommun bedrev ett pilotprojekt för att utveckla tredimensionella stadsmodeller i GIS. För att åstadkomma detta samlades bildinformation in från luften och från marken. Bildinformationen från marken samlades in med särskilda fotograferingsfordon, som fotograferar en 360-graders panoramabild var tionde meter längs med gatunätet. Datainspektionen såg med utgångspunkt från personuppgiftslagens bestämmelser inte något principiellt hinder mot att kommunen använde GIS för att effektivisera sin verksamhet, men bedömde att systemet med tredimensionella stadsmodeller i GIS innebär, åtminstone i princip, att kommunen behandla personuppgifter som kan vara integritetskänsliga. ”Eftersom adresser och fastighetsbeteckningar *i vissa fall* [förf. kursivering] kan utgöra personuppgifter kan systemet sägas innehålla en personuppgiftsanknuten struktur”, skriver Datainspektionen.

Även bild- och ljuduppgifter om fysiska personer utgör personuppgifter (jämför punkt 14 i ingressen till EG-direktivet). Det förutsätter dock att man av bild- eller ljudupptagningen, direkt eller indirekt, kan sluta sig till vilken individ upptagningen avser (EU-domstolens dom den 11 december 2014 i mål C-212/13).

Datainspektionen har ansett att digitala bilder på klotter med beteckningar på en enskild klottrare, s.k. tag, eller ett gäng klottrare, s.k. crew, utgör personuppgifter om polisen kan härleda klottret till en viss person (beslut 2005-08-30, dnr 1020–2005; se också beslut 2006-04-25, dnr 366–2006, och beslut 2011-04-13, dnr 352–2011).

Datainspektionen har vidare ansett att en digital inspelning av en persons röst utgör personuppgifter förutsatt att personen kan identifieras med hjälp av rösten (yttrande 2004-10-06, dnr 1579–2004).

Information som kan hänföras till individer bara i egenskap av medlemmar av en större grupp personer torde inte vara att anse som personuppgifter, t.ex. påståendet ”svenska medborgare har rösträtt i Sverige” eller information om ”aktieägarna i Volvo” eller ”de anställda i Volvo”.[24]

Om uppgifter dock direkt kan hänföras till en begränsad grupp personer, t.ex. en handfull personer med tillgång till en och samma dator eller nätanslutning, att en enskild individ med hjälp av andra uppgifter, t.ex. tjänstgöringslistor, enkelt kan identifieras, kan uppgifterna då betraktas som personuppgifter. Datainspektionen har t.ex. ansett att uppgifter i inpasseringslogg om när en för ett hushåll gemensam elektronisk nyckel använts utgör uppgifter om samtliga medlemmar i hushållet (beslut 2008-07-02, dnr 632–2008). I Finland räcker det enligt en uttrycklig definition i lagen med att uppgifterna kan hänföras till ett hushåll.

---

[24] Sören Öman, Hans-Olov Lindblom, Personuppgiftslagen – en kommentar, Zeteo, kommentaren till 3 § PUL, begreppet personuppgifter.

Även pseudonymiserade personuppgifter, t.ex. krypterade personuppgifter eller andra liknande elektroniska identifikationsinstrument, kan utgöra personuppgifter. Om de kan ”dekrypteras” med en kodnyckel, översättningstabell eller andra medel utgör de personuppgifter. Det är inte nödvändigt att en identifikation har skett för att det ska kunna vara fråga om en personuppgift. Det är fullt tillräckligt att så kan komma att ske.

Datalagskommittén har uttalat att även om ett trafikföretag inte registrerat vem som innehar ett månadskort, kan det vara fråga om en personuppgift eftersom den uppgiften kan finnas registrerad på något annat håll, t.ex. hos den skola eller socialförvaltning som delat ut kortet. I ett sådant fall bedömde Datainspektionen uppgifterna som personuppgifter (beslut 2005-09-09, dnr 857–2005). Jämför också trafikföretags registrering av reseuppgifter vid användning av s.k. e-biljetter (Datainspektionens beslut 2007-10-30, dnr 183–2007, 550–2007 och 1356). Även ett ofullständigt kontokortsnummer som registreras vid köp i butik har ansetts utgöra en personuppgift hos butiken, eftersom informationen tillsammans med information som det kortutfärdande företaget har kan härledes till en individ (Datainspektionens beslut 2009-12-22, dnr 705–2009).

Motsvarande resonemang kan föras beträffande s.k. nätnodsadresser och liknande ”elektroniska identiteter” som den som driver en elektronisk tjänst på t.ex. internet samlar in. Sådana uppgifter om användarna kan nämligen ofta hänföras till en individ med hjälp av uppgifter som användarens internetleverantör har tillgång till.

Datainspektionen anser att s.k. IP-nummer utgör en personuppgift i de fall som någon, t.ex. en internetleverantör, kan hänföra uppgiften till en enskild abonnent eller användare som är en fysisk person (beslut 2005-06-08, dnr 593-2005, beslut 2005-10-13, dnr 1019-2005 och 1318-2005, beslut 2006-12-15, dnr 1631 och 1632-2006 och beslut 2007-05-02, dnr 1625-2006 och 58-2007).[25] I ett fall har Kammarrätten i Stockholm efter överklagande gjort samma bedömning som Datainspektionen (dom 2007-06-08 i mål nr 285-07). Regeringsrätten meddelade inte prövningstillstånd i målet (beslut 2009-06-16 i mål nr 3978–07). Datainspektionen har även ansett att s.k. mac-adresser är personuppgifter (beslut 2015-06-22, dnr 2729–2014).

När syftet med en behandling av uppgifter inte har varit att identifiera enskilda personer har Datainspektionen ansett att inte ens signalementsuppgifter av typen ”man 36–50 år, normalbyggd, hårfärg brunt, frisyr rakt, bakåtkammat med långt i nacken, ansiktsform runt, nationalitet svensk, ögon grå, alldaglig klädsel, tal ljust” utgör personuppgifter (beslut 2005-03-09, dnr 1990–2004). Det aktuella fallet gällde ett datasystem som skulle ge hotellföretag en möjlighet att utbyta upplysningar och varningar och därmed öka uppmärksamheten för vissa företeelser.

Datainspektionen har inte heller ansett att det var fråga om personuppgifter när en kommun informerade på internet om när brottslingar skulle friges (beslut 2000-06-29, dnr 1123–2000). Informationen omfattade uppgifter om att en person

[25] Se dock Daniel Westman, ”Personuppgiftslagen och kampen mot piratkopiering” i Lov & Data 2005 nr 4 s. 7–11) som vänder sig mot Datainspektionens bedömning.

hemmahörande i ett visst område i kommunen och dömd för visst brott snart skulle släppas, men inga direkta namn- eller adressuppgifter.

8.1.2 Överväganden

Embrace är ett verktyg för att registrera brottsliga handlingar och andra otrygghetsskapande händelser, oavsett om de polisanmäls eller inte. Genom att systematiskt registrera dylika händelser kan kunskap vinnas om bakomliggande orsaker till händelserna, och därmed vidta kompensatoriska eller reducerande åtgärder till undvikande av liknande händelse.

En viktig uppgift som ska registreras är platsen för ett brott eller en otrygghetsskapande händelse. Ett krossat fönster i ett bostadshus kräver registrering av gatu- eller fastighetsadress, och kan kompletteras med GPS-koordinater om så behövs för att visa var på byggnaden skadan inträffat. Endast sådana händelser i offentliga miljöer är i fokus, inte händelser som sker i hemmet. Gatu- och fastighetsadresser, liksom GPS-koordinater, är sökbara i Embrace.

Det är tydligt att syftet med Embrace inte är att registrera enskilda personer. Människor är inte i fokus för det brottsförebyggande arbetet, varken brottsoffer eller förövare. Det är händelsen som är av intresse, liksom platsen för densamma. Det skulle tala för att Embrace inte behandlar personuppgifter.

Som framgår av praxisgenomgången har Datainspektionen i något fall ansett att automatiserad behandling av uppgifter som inte syftar till att identifiera personer inte utgör en behandling av personuppgifter, givet att behandlingen inte innefattar några namn- eller adressuppgifter (se avsnitt 8.1.1).

Å andra sidan kan *indirekta uppgifter* i vissa fall utgöra personuppgifter, särskilt uppgifter om *föremål* (fordon, hus, konst m.m.). Föremål tillhör vanligtvis någon, eller är utsatta för eller har ett särskilt inflytande på personer, eller har en sorts fysisk eller geografisk närhet till personer eller andra föremål.

Artikel 29-arbetsgruppen, som var en myndighet inom EU som hade till uppgift att tolka det tidigare dataskyddsdirektivet, beskriver i ett exempel uppgifter om *värdet* för en specifik fastighet.[26] Uppgiften om värdet är en harmlös uppgift. Fastigheten, ett hus, utgör emellertid en ägares tillgångar, och informationen om värdet kan därmed användas för att t.ex. avgöra ägarens skyldighet att betala skatt. I detta sammanhang anser Artikel 29-arbetsgruppen att det inte råder några tvivel om att sådan information bör betraktas som personuppgifter.

Av det redovisade samrådsyttrande rörande Linköpings kommuns GIS-projekt för stadsplanering framgår att systemet innehöll bilder på bl.a. gatuskyltar och fastigheter (se avsnitt 8.1). Även det utgör indirekta uppgifter i vissa fall som kan hänföras till fysiskt levande personer. ”Eftersom adresser och fastighetsbeteckningar i vissa fall kan utgöra personuppgifter kan systemet sägas innehålla en personuppgiftsanknuten struktur”, skriver Datainspektionen i yttrandet.[27]

---

[26] Yttrande 4/2007 om begreppet personuppgifter s. 9.
[27] Datainspektionen samrådsyttrande 2008-04-09, dnr 1070–2007.

Enligt dataskyddsförordningen utgör bl.a. ”lokaliseringsuppgifter” en personuppgift. Med andra ord, möjligheten att identifiera en individ kräver inte hans eller hennes namn. Gatu- och fastighetsadresser har en tydlig koppling till boende på adresserna, och det är inte ett nödvändigt krav för att uppfylla kriterierna för personuppgifter att kopplingen ska ske till en (1) fysisk individ, vilket ju kan vara svårt, utan kravet får anses lägre ställt i den meningen att gatu- och fastighetsadresser kan kopplas till individer till ett hushåll eller till en mindre krets boende.

Artikel 29-arbetsgruppen anför vidare följande:[28]

”*Om identifiering av den registrerade inte ingår i syftet med databehandlingen blir de tekniska åtgärderna för att förhindra identifiering av mycket stor betydelse. Att vidta lämpliga avancerade tekniska och organisatoriska åtgärder för att skydda uppgifterna mot identifiering kan vara det som gör att personerna inte anses identifierbara, med beaktande av alla hjälpmedel som rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person i syfte att identifiera individerna.”*

Begreppet personuppgifter har medvetet fått en bred definition i dataskyddsförordningen, och kanske en ännu bredare tolkning i svensk rätt[29], men har givetvis inte en obegränsad räckvidd. Målet med dataskyddsförordningen är att skydda enskilda individers grundläggande rättigheter och friheter, särskilt deras rätt till privatliv, när det gäller behandling av personuppgifter. Bestämmelserna i regelverken har därför utformats för att gälla i situationer där individens rättigheter kan vara i fara och följaktligen i behov av skydd. Tillämpningsområdet för dataskyddsbestämmelserna bör inte sträckas för långt men man bör inte heller begränsa tolkningen av begreppet personuppgifter mer än nödvändigt.

Embrace registrerar bl.a. gatu- och fastighetsuppgifter. Sådana uppgifter kan i vissa fall kopplas indirekt till fysiskt levande personer. Särskilt när det rör sig om adresser hänförliga till hyres- eller bostadsrätter samt villor. Huruvida Embrace hanterar personuppgifter i dataskyddsförordningens mening, trots att sådana avsikter inte finns, måste ställas i relation till risken för enskilda fri- och rättigheter.

Det är t.ex. inte uteslutet att uppgifterna i Embrace kan användas av försäkringsbolag för riktad marknadsföring av försäkringsskydd till utsatta områden och boende där genom att ta del av fastighetsregister eller boendeförteckningar i trapphus, om uppgifterna skulle vara tillgängliga för dessa aktörer. Det kan inte heller uteslutas att lika väl som Embrace används i brottsförebyggande syfte, en illvillig person kan nyttja samma information, om uppgifterna vore tillgängliga eller spreds obehörigen, för att utföra brottslig verksamhet mot de fysiska personer i specifika hus eller bostäder som drabbats tidigare p.g.a. brister i den fysiska miljön som bäddar för brott.

Embrace Safety AB har inte för avsikt att ”sälja” information i Embrace till tredje part. Detta är därför spekulativa eller hypotetiska bedömningar, men inte helt

---

[28] Yttrande 4/2007 om begreppet personuppgifter s. 17.

[29] Daniel Westman, ”Personuppgiftslagen och kampen mot piratkopiering” i Lov & Data 2005 nr 4 s. 7–11).

orealistiska. Poängen dock med exemplen är att uppgifterna i Embrace kan nyttjas för att identifiera enskilda personer och exponera dem för medvetna handlingar som inkräktar på deras privatliv.

I sammanhanget ska också framhållas fritextrutorna i Embrace samt vilka åtgärder Embrace Safety AB vidtagit för att förhindra att användare i organisationer som nyttjar tjänsten registrerar direkta personuppgifter i densamma. Som redovisas i avsnitt 2.2 är Embrace inte designat för att registrera enskilda individer utan bara brottsrelaterade och andra otrygghetsskapande händelser. Fritextrutor innebär alltid risk för behandling av personuppgifter. Embrace framhåller att användare får utbildning i riskerna med registrering av personuppgifter, och att utsedda administratörer ”rensar” fritext från uppenbara individuppgifter. Vidare kan inte uppgifter som registreras i Embrace hos en aktör lämnas ut till den gemensamma lokala problembilden (Embrace Insight) utan att först en anställd administratör hos organisationen har granskat uppgifterna och ”godkänt” dem för gemensam delning med andra aktörer. Det är inte tekniskt möjligt för ”vanliga” användare att lämna ut uppgifter till Embrace Insight.

Som framhållits kan man genom tekniska och administrativa åtgärder i ett datasystem helt eliminera risken för behandling av personuppgifter, och därmed inte behöva beakta dataskyddsreglerna eftersom det inte finns några risker för enskilda fri- och rättigheter. Embrace är dock beroende av exakta platser och geodata för att kunna bygga statistik och se mönster över förseelser och brott inom ett geografiskt område. De skulle således vara kontraproduktivt med sådana långtgående mekanismer i Embrace.

Vid en sammantagen bedömning, och med beaktande av en försiktighetsprincip, får Embrace anses i vissa fall behandla personuppgifter. Men inte alltid. Händelser som inträffar på allmänna platser, t.ex. ett torg, utgör inte personuppgifter eftersom dessa händelser svårligen kan hänföras indirekt till enskilda individer.

Tekniska och administrativa mekanismer finns emellertid på plats i tjänsten för att förhindra registrering och utlämnande av uppgifter om enskilda individuppgifter. De får anses godtagbara ur dataskyddsförordningens och brottsdatalagens perspektiv för att värna om enskildas personuppgifter.

Det erinras att det är Embrace Safety AB:s kunder som ansvarar själva för att individuppgifter inte registreras i tjänsten i rollen som personuppgiftsansvariga (se avsnitt 8.4). Embrace Safety AB:s roll är att tillhandahålla utbildning åt kunderna om persondataskyddsreglerna och att arbeta aktivt med mekanismer som förhindrar registrering av enskilda fysiska personer. Det skulle tala för att fritextrutorna fortsättningsvis skulle kunna användas i Embrace.

Embrace Safety AB rekommenderas emellertid att överväga att ta bort dessa rutor med hänsyn till risken för registrering av *känsliga personuppgifter*, vilka inte egentligen behövs i tjänsten och som kräver särskilda lagliga grunder (se avsnitt 8.6 och 8.7).

8.2 Är Embrace ett register som omfattas av dataskyddsregleringen?

Bedömning: Embrace är ett datoriserat register och omfattas därmed av dataskyddsförordningen, brottsdatalagens respektive polisdatalagens bestämmelser. Vilka av dessa författningar som blir tillämplig på Embrace beror på vem som använder tjänsten, se avsnitt 8.3.

I det föregående konstateras att Embrace behandlar personuppgifter. Ytterligare kriterier ska emellertid vara uppfyllda för att regelverket om persondataskydd ska vara tillämpliga på Embrace.

Enligt art. 2.1 dataskyddsförordningen är förordningen tillämplig på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Av skäl 15 framgår att akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av förordningen. Brottsdatalagen har samma tillämpningsområde (1 kap. 3 §).

Tillämpningsområdet för både dataskyddsförordningen och brottsdatalagen är detsamma således. Frågan är om Embrace omfattas av dessa kriterier, och därmed av de bestämmelser som ska iakttas om persondataskydd.

Enligt Datalagskommittén är det klart att behandling i datorer av personuppgifter som finns i datorformat (i binär form, såsom ettor och nollor, eller motsvarande) – inklusive överföringen av personuppgifter till sådant format – som regel bör anses som automatiserad behandling. Så snart en personuppgift har kommit in i en dator eller motsvarande maskin skulle det alltså som regel vara fråga om sådan automatiserad behandling som omfattas av lagen.

Embrace är ett datorbaserat system för registrering och analys av förseelser och brottsliga handlingar. Bl.a. registreras geografiska data, adress- och fastighetsuppgifter, fotografier och andra detaljer om händelsen. Sådana uppgifter är vidare sökbara. Embrace omfattas därmed idag av dataskyddslagens, brottsdatalagens respektive polisdatalagens (2010:361) bestämmelser. Vilken av dessa författningar som blir tillämplig på olika aktörers användning av Embrace övervägs i avsnitt 8.3.

8.3 Är dataskyddsförordningen eller brottsdatalagen tillämplig på Embrace?

Bedömning: Brottsdatalagen är tillämplig enbart på myndigheter med brottsbekämpande uppdrag eller som utövar myndighet samt andra aktörer med motsvarande uppdrag.

En tydlig målgrupp för Embrace är bl.a. kommuner och Polismyndigheten. Kommuner har inte ett brottsbekämpande uppdrag eller utövar myndighet för de syften som brottsdatalagen anger. När kommunerna använder Embrace ska de således iaktta dataskyddsförordningens och dataskyddslagens bestämmelser.

Polismyndigheten däremot ska beakta polisdatalagen, och fr.o.m. den 1 januari 2019 beakta den nya lagen om polisens behandling av personuppgifter inom brottsdatalagens område när myndigheten använder Embrace, och i övrigt beakta brottsdatalagen. I nuläget bedöms polisens personuppgiftsbehandling ha stöd i den nuvarande polisdatalagens bestämmelser. Den preliminära bedömningen är att personuppgiftsbehandlingen i Embrace inom ramen för polisens brottsförebyggande arbete alltjämt kommer att vara tillåten enligt lagen om polisens behandling av personuppgifter inom brottsdatalagens område fr.o.m. den 1 januari 2019 när den lagen träder i kraft.

Informationsöverföring av uppgifter i Embrace till andra myndigheter när Polismyndigheten använder tjänsten behandlas i andra delar av denna framställning, se avsnitt 8.6.

Enligt art. 2.2 dataskyddsförordningen ska förordningen inte tillämpas på behandling av personuppgifter som bl.a. ”behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten”. Behandlas personuppgifter av ”behöriga myndigheter” för dylika ändamål ska i stället nationella dataskyddsbestämmelser som fattas med stöd av det nya brottsdatadirektivet tillämpas.

Som redovisas i kapitel 7 trädde en ny brottsdatalag i kraft den 1 augusti 2018.

Av intresse för Embraces vidkommande, som registrerar bl.a. uppgifter om brottshändelser, är vilken lagstiftning som är tillämplig på tjänsten – dataskyddsförordningen eller brottsdatalagen.

Ett grundläggande krav för att brottsdatalagen ska vara tillämplig är att den som behandlar personuppgifterna är en ”behörig myndighet” i lagens mening och att behandlingen görs för något av de syften som anges där. Av definitionen för ”behörig myndighet” i brottsdatalagen framgår att det rör sig om

1. En myndighet som har till uppgift att

a) förebygga, förhindra eller upptäcka brottslig verksamhet,

b) utreda eller lagföra brott,

c) verkställa straffrättsliga påföljder, eller

d) upprätthålla allmän ordning och säkerhet, eller

2. en annan aktör som utövar myndighet för något av de syften som anges i punkten 1.

Det rör sig alltså om sådana myndigheter som fullgör arbetsuppgifter inom lagens tillämpningsområde och andra aktörer som utövar myndighet i samma syften som är behöriga (se avsnitt 6.1). Är den som behandlar personuppgifterna inte en ”behörig myndighet” – per definition – gäller inte brottsdatalagen för personuppgiftsbehandlingen utan i stället dataskyddsförordningen samt dataskyddslagen (se avsnitt 7.3).

Många myndigheter och andra aktörer är skyldiga att anmäla om det uppstått misstanke om brott. En sådan skyldighet medför inte att anmälaren ska betraktas som

behörig myndighet i brottsdatalagens mening, om anmälaren varken har ett brottsbekämpande uppdrag eller utövar myndighet för de syften som lagen omfattar.[30]

Det förhållandet att någon som har fått tillstånd att sätta upp en övervakningskamera t.ex. i en bank eller butikslokal i syfte att förebygga, avslöja eller utreda brott innebär inte heller att behandlingen av de personuppgifter som erhålls genom övervakningen görs av en behörig myndighet i brottsdatalagens mening. Företaget eller personen i fråga ägnar sig nämligen inte åt myndighetsutövning.[31]

En tydlig målgrupp för Embrace är bl.a. kommuner och Polismyndigheten. Vad beträffar först kommuner, så har de inte ett *brottsbekämpande* uppdrag eller utövar myndighet för de syften som brottsdatadirektivet anger. Det innebär att kommuner som använder Embrace ska iaktta dataskyddsförordningens bestämmelser. Motsvarande bedömning gäller eventuellt för andra aktörer som använder Embrace, t.ex. bostads- och fastighetsbolag. Sådana aktörer ska beakta dataskyddsförordningens och dataskyddslagens bestämmelser – inte brottsdatalagens.

Beträffande sedan Polismyndigheten så har den myndigheten, till skillnad från kommuner, ett tydligt brottsbekämpande uppdrag, men också brottsförebyggande arbetsuppgifter. Enligt 2 § polislagen (1984:387) hör till Polismyndighetens uppgifter bl.a. att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten. Enligt förslaget till brottsdatalag avses med en behörig myndighet en myndighet som har till uppgift att (bl.a.) förebygga, förhindra eller upptäcka brottslig verksamhet.

Det innebär att polisen inte ska tillämpa dataskyddsförordningen utan i stället personuppgiftslagen när den myndigheten behandlar personuppgifter i Embrace. Att personuppgiftslagen fortfarande gäller för Polismyndighetens personuppgiftsbehandling framgår av dataskyddslagens övergångsbestämmelser. Först den 1 januari 2019 ska Polismyndigheten i stället beakta brottsdatalagen när myndigheten får en ny registerförfattning (se nedan). Brottsdatalagen är subsidiär i förhållande till specialreglering kring persondataskydd.[32] En sådan specialreglering är polisdatalagen (2010:361).

Syftet med polisdatalagen är att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin brottsbekämpande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Av 7 § polisdatalagen framgår bl.a. att personuppgifter får behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet.

Polisdatalagen är således tillämplig på Embrace när polisen använder verktyget, och kompletteras av personuppgiftslagen t.o.m. 31 december 2018. Som nämnts bl.a. i avsnitt 7.2 har regeringen föreslagit en ny lag om polisens behandling av personuppgifter inom brottsdatalagens område som beräknas träda i kraft den 1

[30] Prop. 2017/18:232 s. 111.
[31] Ib.
[32] Ib. s. 77.

januari 2019. Då ska Polismyndigheten beakta brottsdatalagen i stället för personuppgiftslagen.

Eftersom Polisens nya dataskyddsreglering är än så länge ett förslag till riksdagen är det vanskligt att i nuläget analysera Embrace tillåtlighet enligt den lagen. Vissa verkställighetsföreskrifter och andra detaljer kommer att meddelas av regeringen i en förordning. Såvitt kan bedömas med utgångspunkt från nuvarande regelverk så utgör Embrace helt klart en tillåten behandling av personuppgifter enligt polisdatalagen, och torde så förbli när den nya lagen om polisens behandling av personuppgifter inom brottsdatalagens område beräknas träda i kraft 1 maj 2018 efter riksdagens godkännande. Polismyndighetens användning av Embrace berörs längre fram i denna framställning, t.ex. vid informationsöverföring från polisen till andra aktörer som använder Embrace inom ramen för en samverkan mot brott samt personuppgiftsansvaret för uppgifterna i tjänsten.

Den omständigheten att någon som inte har brottsbekämpande, lagförande, straffverkställande eller ordningshållande uppdrag ges tillgång till ett register som förs av en myndighet med ett brottsbekämpande uppdrag innebär inte att den förra ska betraktas som behörig myndighet. Det gäller även den som på annat sätt får del av uppgifter om lagöverträdelser. Den som får tillgång till domar eller till vissa uppgifter ur t.ex. belastningsregistret eller registret över tillträdesförbud blir alltså inte en behörig myndighet av det skälet.[33] För att brottsdatalagen ska vara tillämplig krävs, som sagt, att uppgifterna i fråga behandlas av en behörig myndighet för något av de syften som lagen anger.

Det sagda innebär att om Polismyndigheten använder Embrace, och tillåter en kommun att få ta del av uppgifterna däri, detta inte medför att kommunen ”smittas” av brottsdatalagens bestämmelser utan kommunen fortsätter tillämpa dataskyddsförordningens bestämmelser för sin behandling som kommunen utför i Embrace. Detta under förutsättning att det rör sig om personuppgifter, vilket kommer att vara fallet undantagsvis.

8.4 Vem är personuppgiftsansvarig för Embrace?

Bedömning: Embraces kunder är personuppgiftsansvariga för sin användning av personuppgifter i tjänsten, t.ex. kommuner, Polismyndigheten samt bostads- och fastighetsföretag. Det beror på att Embrace är en molntjänst. Var och en av kunderna bedöms ansvara också för sina uppgifter som man tillför den gemensamma lokala problembilden i Embrace Insight. Embrace Safety AB hanterar personuppgifter, i de fall sådana uppgifter förekommer i Embrace, i rollen som personuppgiftsbiträde.

Personuppgiftsbiträden har ett begränsat juridiskt, självständigt ansvar för de personuppgifter man behandlar i rollen som personuppgiftsbiträde. Bl.a. ansvarar Embrace Safety AB självständigt för att säkerställa ett adekvat skydd för eventuella personuppgifter i tjänsten samt rapportera personuppgiftsincidenter utan onödigt dröjsmål till kunden.

[33] Ib. s. 113.

Inom en kommun är alltid en nämnd eller kommunstyrelsen personuppgiftsansvarig. Beträffande osjälvständiga nämnder, t.ex. utförarnämnder av viss verksamhet eller IT, är ofta en annan, självständig nämnd personuppgiftsansvarig för den osjälvständiga nämndens personuppgiftsbehandling. Embrace Safety AB bör vara uppmärksam på detta förhållande när personuppgiftsbiträdesavtal ska tecknas med en förvaltning/nämnd som vill använda Embrace. Det är ett krav enligt dataskyddsförordningen och brottsdatalagen att ett skriftligt avtal ska tecknas när en aktör behandlar personuppgifter för en personuppgiftsansvarigs räkning.

Embrace utvecklas av Embrace Safety AB. Målgrupperna för datorsystemet är främst polisen, kommuner och fastighetsföretag. Frågan är vem av dessa aktörer som ska bära det juridiska ansvaret för personuppgiftsbehandlingen i Embrace.

Med *personuppgiftsansvarig* avses enligt dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt, (art. 4.7). Definitionen på personuppgiftsansvarig i brottsdatalagen har samma lydelse. Någon skillnad i innebörden av begreppet för personuppgiftsansvarig mellan PUL:s definition och det nya EU-regelverket finns inte.

Den personuppgiftsansvarige kan överlåta den faktiska behandlingen av personuppgifter, men personuppgiftsansvaret kan aldrig överlåtas. Det är alltid den personuppgiftsansvarige som ytterst svarar för att personuppgiftslagen följs och att de registrerade behandlas korrekt. Ansvaret är skadeståndssanktionerat. Vidare kan personuppgiftsansvariga dessutom drabbas av vitessanktioner som är tämligen höga. Det är en följd av en ökad betoning på ansvaret för persondataskyddet i dataskyddsförordningen och brottsdatadirektivet. Det är viktigt ur ett integritetsperspektiv att det finns någon som är personuppgiftsansvarig och att det klart framgår utåt vem som bär ansvaret, så att de registrerade kan ta tillvara sina rättigheter i samband med behandlingen.

Personuppgiftsansvaret kan bäras av en part eller delas av flera. En konstruktion med delat personuppgiftsansvar kan dock vara riskabel om alla aktörer kan hantera all information i systemet, eftersom parterna i så fall är solidariskt ansvariga om någon av dem skulle använda uppgifterna på ett olagligt sätt. Det kan också uppstå tveksamheter om vilket lands personuppgiftslag som är tillämplig när flera aktörer är personuppgiftsansvariga. Det finns visst utrymme att avtala om personuppgiftsansvaret, men det går aldrig att avtala bort ett sådant ansvar; det är den som faktiskt bestämmer över personuppgiftsbehandlingen som är personuppgiftsansvarig.

I vissa fall är personuppgiftsansvaret bestämt i författning. Enligt t.ex. polisdatalagen är Polismyndigheten personuppgiftsansvarig för sin behandling av personuppgifter.

Om personuppgiftsansvaret bärs av en eller flera parter, kan övriga inblandade aktörer utgöra personuppgiftsbiträden. Ett *personuppgiftsbiträde* enligt dataskyddsförordningen är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning (art. 4.8). Motsvarande definition finns i brottsdatalagen.

Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges egen organisationen och kan vara antingen en fysisk eller en juridisk person. Om den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, får biträdet endast behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner. Ett skriftligt avtal eller någon annan form av rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt måste i sådant fall upprättas. Det framgår av både dataskyddsförordningen och brottsdatalagen. I avtalet eller rättsakten ska det bl.a. särskilt föreskrivas föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter anges. I det avtalet eller den rättsakten ska det vidare finnas dokumenterade instruktioner till personuppgiftsbiträdet.

Enligt dataskyddsförordningen och brottsdatalagen har personuppgiftsbiträden fått vissa skyldigheter som innebär att även de kan drabbas i viss utsträckning av skadeståndsansvar och vitessanktioner. Bl.a. ska personuppgiftsbiträden säkerställa skyddet för personuppgifter, följa den personuppgiftsansvariges instruktioner, rapportera personuppgiftsincidenter till den personuppgiftsansvarige utan onödigt dröjsmål och föra register över kategorier av personuppgifter som biträdet behandlar åt personuppgiftsansvariga.

Enligt Embrace Safety AB avser bolaget att tillhandahålla Embrace som en molntjänst. Embrace Safety AB avser själva inte att bedriva någon brottsförebyggande verksamhet utan enbart tillhandahålla den aktuella digitala tjänsten Embrace.

Det innebär att den som köper tjänsten för att använda den för lokalt och kunskapsbaserat brottsförebyggande arbete i den egna verksamheten sannolikt är personuppgiftsansvarig.

Mot detta kan man invända att personuppgiftsbehandling vid applikationsuthyrning eller molntjänster kännetecknas av att det är leverantören av en molntjänst snarare än kunden som i praktiken har den faktiska kontrollen över hur personuppgifter behandlas inom ramen för tjänsten, dvs. att Embrace Safety AB skulle vara personuppgiftsansvarig för andra aktörers användning av verktyget. Trots detta fann Datainspektionen i ett tillsynsprojekt 2011 av molntjänster som utmynnade i ett flertal tillsynsbeslut, *att den som använder molnleverantörer är alltid personuppgiftsansvarig*.

Sammanfattningsvis är det Embrace Safety AB:s kunder som är personuppgiftsansvariga för sin användning av personuppgifter i tjänsten, t.ex. kommuner, Polismyndigheten och fastighetsföretag. Det beror på att Embrace är en molntjänst. Var och en av kunderna bedöms ansvara också för sina uppgifter som man tillför den gemensamma lokala problembilden i Embrace Insight. Embrace Safety AB hanterar personuppgifter, i de fall sådana uppgifter förekommer i tjänsten, i rollen som personuppgiftsbiträde.

Beträffande kommuner erinras att varje nämnd är en myndighet, och att personuppgiftsansvaret är knutet till nämnden. Detta under förutsättning att nämnden har en viss självständighet. Det är inte alldeles självklart. I många fall finns utförarnämnder, och beställarnämnder. Det kan förhålla sig så att en nämnd är personuppgiftsansvarig för en osjälvständig nämnds personuppgiftsbehandling, om den förstnämnda nämnden har bestämt ändamålen med och medlen för personuppgiftsbehandling i en viss verksamhet. Ett exempel kan vara kommunstyrelsen i en mindre kommun som via ett arbetsutskott bestämmer utformningen av IT-system som köps in eller hyrs in för att användas i hela den kommunala förvaltningen.

Embrace bör vara uppmärksam på detta förhållande när personuppgiftsbiträdesavtal ska tecknas med en förvaltning/nämnd som vill använda Embrace.

8.5 Grundläggande principer för personuppgiftsbehandling

Det är de personuppgiftsansvariga, dvs. Embrace Safetys kunder, som ska iaktta de grundläggande principerna för dataskydd i dataskyddsförordningen respektive brottsdatalagen vid all personuppgiftsbehandling i Embrace, men det utesluter inte att Embrace Safety AB erbjuder stöd och utformar tjänsten så att kunderna kan leva upp till dataskyddsprinciperna.

Om personuppgifter behandlas med stöd av en laglig grund (se avsnitt 8.6), men någon av de grundläggande dataskyddsprinciperna inte är iakttagna, riskerar personuppgiftsbehandlingen att betraktas som otillåten.

Dataskyddsförordningen innehåller sex grundläggande dataskyddsprinciper (art. 5.1). De ska alltid iakttas vid strukturerad behandling av personuppgifter. Motsvarande principer finns i brottsdatadirektivet. I det följande uppehåller sig framställningen vid dataskyddsförordningens principer. Dessa är följande:

1. Laglighet, korrekthet, öppenhet
2. Ändamålsbegränsning
3. Uppgiftsminimering
4. Korrekthet
5. Lagringsminimering
6. Integritet och konfidentialitet

En nyhet är kravet i art. 5.2. Den personuppgiftsansvarige ska ansvara för och kunna ”visa” att de grundläggande principerna efterlevs. Det är ett uttryck för ansvarsprincipen. Den innebär att man ska inte bara följa regelverket utan också kunna visa att man gör det!

Det är mot den bakgrunden dataskyddsförordningen innehåller bestämmelser om dataskyddskonsekvensbedömningar och förhandssamråd med tillsynsmyndigheten, som ska tillämpas om behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (art. 35 och 36).

Behandlas personuppgifter med stöd av en laglig grund, men någon av de grundläggande principerna inte är iakttagna, riskerar personuppgiftsbehandlingen att betraktas som otillåten. Det saknar betydelse att personuppgiftsbehandlingen har stöd i en registerförfattning. En personuppgiftsansvarig ska vidare, som sagt, kunna ansvara för och ”visa” att man uppfyller de sex principerna (art. 5.2).

De principer som torde krävas särskild uppmärksamhet i Embrace är principerna om

- Öppenhet
- Ändamålsbegräsning
- Uppgiftsminimering

Enligt art. 5.1 b dataskyddsförordningen ska personuppgifter samlas in för *särskilda, uttryckligt angivna och berättigade ändamål* och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (principen om ändamålsbegränsning och finalitetsprincipen). Ändamålet med behandlingen bestämmer sedan hur den personuppgiftsansvarige får använda de redan insamlade uppgifterna.

Såvitt kan bedömas är ändamålet med Embrace brottsförebyggande lokalt arbete genom

1. Kartläggning av förseelser och brott, såväl polisanmälda som icke-polisanmälda, varvid uppgifter om platsen för händelsen registreras, men inte individuppgifter
2. Analys av registrerade uppgifter och med stöd av befintliga öppna kunskapskällor och register
3. Insatser för att reducera eller eliminera nya, liknande förseelser eller brott
4. Uppföljning av brott och insatser
5. Återkoppling till berörda avnämare

Ändamålet kan behöva formuleras skarpare av de personuppgiftsansvariga, som ju har den rättsliga skyldigheten att iaktta de grundläggande principerna i dataskyddsförordningen respektive brottsdatalagen.

Vidare gäller enligt art. 5.1 c att de personuppgifter som behandlas måste vara *adekvata och relevanta* i förhållande till ändamålen med behandlingen och att *inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen* (principen om uppgiftsminimering). Den personuppgiftsansvarige måste med andra ord se till att behandlingen av personuppgifter i Embrace har ett i förväg bestämt och berättigat ändamål som dessutom är sakligt grundat i verksamheten.

Behandlingen får inte heller *utföras godtyckligt eller kränkande eller på ett sätt som strider mot lag eller god sed samt vara transparent för de registrerade* (art. 5.1 a; principen om laglighet, korrekthet och öppenhet). Det får aldrig komma som en överraskning för registrerade i Embrace att de förekommer i verktyget och används för visst eller vissa ändamål.

Det är alltså Embrace Safety AB:s kunder som ska iaktta dessa grundläggande principer. Givetvis har Embrace Safety AB ett inflytande över kundernas efterlevnad av dessa principer genom att utforma tjänsten på ett sådant sätt att principerna kan efterlevas eller levas upp till.

Ett exempel får åskådliggöra Embrace Safety AB:s möjligheter att hjälpa sina kunder att följa de grundläggande principerna.

Det finns en risk att kunderna kan komma att hantera olika former av överskottsinformation, dvs. personuppgifter som inte är adekvata och relevanta för ändamålet eller ändamålen med behandlingen i Embrace. Personer riskerar t.ex. att hamna på bild i systemet i onödan när bilder tas av brottsutsatta allmänna platser.

För att behandlingen inte ska riskera att strida mot dataskyddsförordningen, eller för den delen polisdatalagen och brottsdatalagen, måste Embrace vidta åtgärder för att minimera förekomsten av personuppgifter i systemet. Detta kan åstadkommas på flera sätt, t.ex. genom att tillhandahålla stöd för att pixla ev. personer, alltså manuell avidentifiering, som förekommer på bilderna samt utbildning för användare. Bildupplösningen bör dessutom inte vara högre än vad situationen kräver. Administratörens genomgång av fritextrutor för att säkerställa att inga personuppgifter förekommer där i onödan är också en åtgärd. Kunderna själva kan vidare fotografera vid tidpunkter på dygnet då så få personer som möjligt vistas på den allmänna platsen där en förseelse eller en brottslig handling begåtts.

8.6 Rättslig grund

Bedömning: Kommuner ansvarar enligt författning för ett flertal verksamheter som har brottsförebyggande effekt. Kommuner har vidare en nyckelroll i regeringens nya nationella brottsförebyggande program – Tillsammans mot brott (2017). Polisen är helt beroende av kommunerna för sin brottsförebyggande verksamhet.

Mot den bakgrunden får kommuner lagligen behandla personuppgifter i Embrace, i de fall sådana uppgifter förekommer i tjänsten, för att det är nödvändig för att kunna utföra en *arbetsuppgift av allmänt intresse* (6.1 e dataskyddsförordningen samt 2 kap. 4 § dataskyddsförordningen). Kommunen behöver således inte inhämta ett samtycke av enskilda personer i de fall deras personuppgifter behandlas i Embrace.

Polismyndigheten bedöms också lagligen få behandla personuppgifter i Embrace med stöd av polisdatalagen och personuppgiftslagen, som gäller för polisens verksamhet t.o.m. 31 december 2018. Det kan röra sig om personuppgifter som ursprungligen samlats in i den polisiära verksamheten, t.ex. brottsanmälningar i RAR

(Rationell anmälningsrutin), varav vissa uppgifter överförs till polisens egen instans av Embrace.

Polisen bedöms vidare med stöd av polisdatalagen lagligen få behandla personuppgifter i den egna instansen av Embrace för att lämna ut dem till den gemensamma problembilden i Embrace (Embrace Insight), där andra samverkande, behöriga aktörer, t.ex. myndigheter (kommuner), kan ta del av uppgifterna. Även privata aktörer, t.ex. bostads- och fastighetsbolag, kan vara mottagare av sådana uppgifter med stöd av polisdatalagen. Vad beträffar först mottagande myndigheter (kommuner) finns uttryckligt lagstöd för utlämnandebehandlingen i polisdatalagen. Beträffande sedan privata aktörer får polisen efter en oförenlighetsprövning lämna ut sådana uppgifter. Utlämnandebehandlingen bedöms – inom ramen för ett lokalt brottsförebyggande arbete eller en samverkansöverenskommelse med stöd av Embrace - inte vara oförenlig med de ändamål för vilka polisen ursprungligen samlar in uppgifterna.

Merparten av polisens uppgifter som överförs till den gemensamma problembilden i Embrace bedöms dock inte utgöra personuppgifter i brottsdatalagens mening eftersom de inte kan hänföras till en fysisk levande person utan enbart till platser. Varken polisdatalagen eller brottsdatalagen är alltså tillämpliga på sådana uppgifter, och polisen kan fritt lämna ut dem till andra behöriga mottagare i det lokala och gemensamma brottsförebyggande arbetet.

Personuppgifter kan uppstå i form av gatu- och fastighetsadresser, vilka indirekt kan härledas till en eller flera individer som bor på adressen eller fastigheten. Även sådana uppgifter bedöms emellertid polisen kunna, med stöd av polisdatalagen, lagligen få lämna ut till exempelvis privata aktörer.

En del i Polismyndighetens laglighetsprövning avseende utlämnandebehandling av personuppgifter är att kontrollera att sekretess inte lägger hinder i vägen för ett utlämnande till andra mottagare i Embrace. Sekretess behandlas i avsnitt 8.7.

Användare inom näringslivet bedöms lagligen kunna behandla personuppgifter, i de fall sådana förekommer i Embrace, efter en *intresseavvägning* (se 6.1 f dataskyddsförordningen). Bostads- och fastighetsföretag hör klart till den kategorin och får anses ha ett berättigat intresse av att behandla personuppgifter i Embrace med hänsyn till deras påverkansmöjligheter för en trygghetsskapande miljö, varvid intresset för att skydda enskilda personliga integritet får ge vika. Andra privata aktörer måste göra en egen laglighetsprövning av Embrace och utröna den lagliga grunden för personuppgiftsbehandling, se avsnitt 8.4.

Kommunala bostads- och fastighetsbolag utgör inte myndigheter i lagens mening, men kan åberopa samma lagliga grund som kommunen, dvs. utförande av ”arbetsuppgifter av allmänt intresse” (6.1 e samt 2 kap. 4 § i dataskyddsförordningen) eftersom dessa bolag lyder under kommunal styrning och tillhandahållande av bostäder är av allmänt intresse.

Embrace innehåller inte, och ska inte innehålla *känsliga personuppgifter*, t.ex. uppgift om etnicitet, religionstillhörighet eller hälsa. Sådana uppgifter kräver

särskilda lagliga grunder för registrering. Det erinras dock att Embrace har fritextrutor. I fritextrutorna öppnar Embrace upp för registrering av sådana uppgifter.

Ett alternativ är att ta bort fritextrutorna helt och hållet. Ett annat alternativ är att bygga in mekanismer i Embrace som förhindrar sådan registrering. I nuläget finns – såvitt kan bedömas – godtagbara tekniska och administrativa funktioner på plats i Embrace som ska förhindra att individuppgifter och känsliga personuppgifter förekommer hos de enskilda användarna eller lämnas ut till den gemensamma lokala problembilden.

En av frågorna som ska besvaras är med vilken *rättslig grund* personuppgifter får behandlas i Embrace. Vidare frågas om en myndighet får dela information i Embrace med privata aktörer, t.ex. att polisen delar information om händelser med ett kommunalt bostadsbolag, under förutsättning att det finns en samverkan mellan bostadsbolaget och polisen? Dessa frågor behandlas i detta avsnitt.

I 6.1 dataskyddsförordningen finns en uppräkning av i vilka fall behandling av personuppgifter är tillåten. Av brottsdatadirektivet, som ska genomföras i en ny, föreslagen brottsdatalag, framgår av art. 1.1 att det direktivet är tillämpligt enbart på ”behöriga myndigheters” behandling av personuppgifter avseende brottsbekämpning, lagföring och verkställighet av dom samt allmän säkerhet.

I det följande behandlas först rättslig grund för kommuner och andra aktörer som vill använda Embrace. Och därefter Polismyndighetens användning.

8.6.1 Rättslig grund för kommuner m.fl.

Utgångspunkten enligt dataskyddsförordningen är att all behandling av personuppgifter är förbjuden. I undantagsfall ”öppnar” förordningen för viss behandling av personuppgifter. Man kan beskriva dessa undantag som fallsituationer.

Ett kriterium för alla dessa fallsituationer utom i ett fall – samtycke – är att personuppgiftsbehandlingen är *nödvändig*, dvs. att det finns ett behov av att behandla personuppgifterna. Är detta nödvändighetskrav inte uppfyllt, är personuppgiftsbehandlingen otillåten.

Enligt art. 6.1 dataskyddsförordningen är behandling endast laglig om och i den mån som åtminstone ett av följande fall är uppfyllt:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Av andra stycket i art. 6.1 framgår att fallsituationen f (intresseavvägning) *inte gäller för behandling som utförs av offentliga myndigheter* när de fullgör sina uppgifter. Grunden intresseavvägning kan således inte åberopas av en kommun för att behandla personuppgifter i Embrace.

Som nämnts i det föregående ställs relativt höga krav på samtycke för behandling av personuppgifter. Det står givetvis de personuppgiftsansvariga, t.ex. kommuner, fritt att behandla personuppgifterna i Embrace med stöd av samtycke från de registrerade, men det är inte att rekommendera. Ett samtycke ska vara frivilligt, särskilt, otvetydigt och informerat. Den personuppgiftsansvarige ska kunna ”visa” att dessa krav är uppfyllda. Finns det en annan rättslig grund i art. 6.1 som är tillämplig, rekommenderas att den används som stöd för personuppgiftsbehandlingen.

För att kunna närmare bestämma vilken av grunderna i art. 6.1 som kan åberopas av en kommun för sin personuppgiftsbehandling i Embrace (med undantag för den lagliga grunden samtycke respektive intresseavvägning), tarvar kommunens brottsförebyggande arbete och uppgifter en närmare granskning.

Vad menas med begreppet förebygga? Hur ”förebygga” ska förstås har betydelse för vad som ska samordnas. I fråga om kommunerna gäller det vad deras ansvar närmare bestämt omfattar, sett i ljuset av andra myndigheters och organisationers ansvar.

Vikten av att klargöra vad som ligger i begreppet förebygga kan illustreras av att Riksrevisionen (2010) riktat kritik mot polisen och bl.a. menat att det finns en otydlighet i vad brottsförebyggande arbete är för något. Samtidigt är det förebyggande arbetet en av de mest centrala punkterna i polislagen (1984:387).

För all möjlig brottslighet saknar kommunen ett ansvar, en skyldighet att motverka. Några undantag finns dock (se nedan). Det gäller bland annat ungdomar som hamnar i brott. Däremot kan det ligga i medborgarnas intresse att kommunen engagerar sig för att förebygga brott. Då finns ingen skyldighet, men insatser inom vissa gränser kan ligga inom ramen för den kommunala kompetensen, dvs. att tillgodose ”allmänintresset”.

Kommuner och landsting får nämligen, enligt 2 kap. 1 § kommunallagen (2017:725), själva ha hand om sådana angelägenheter av allmänt intresse som har anknytning till kommunens eller landstingets område eller deras medlemmar och som inte ska handhas enbart av staten, en annan kommun, ett annat landsting eller någon annan. *Allmänintresset* och *lokaliseringsprincipen* kan noteras, liksom att angelägenheten inte ska handhas enbart av staten.

För att kommunerna och landstingen själva ska få ha hand om en angelägenhet krävs att det är av allmänt intresse att så sker. Om det med hänsyn till arten av ett visst ändamål anses vara av allmänt intresse att en kommun eller ett landsting främjar det ändamålet, är de berättigade till det även om åtgärden kommer bara en mindre del av kommunens eller landstingets område eller ett mindre antal av medlemmarna direkt till godo. Allmänintresset får bedömas med utgångspunkt i om det är lämpligt, ändamålsenligt, skäligt osv. att kommunen eller landstinget befattar sig med angelägenheten.[34]

Lokaliseringsprincipen innebär i grunden att en kommunal åtgärd måste vara knuten till kommunens eller landstingets eget område eller dess invånare för att den ska anses laglig.

Samtidigt är det Polismyndigheten som enligt polislagen har ansvaret för att förebygga brott. För uppgifter som ska ”handhas enbart av staten” gäller nämligen inte den kommunala kompetensen (2 kap. 2 § KL). Regeringen har dock i policybetonade dokument uttryckt en tämligen vid syn på kommunernas möjligheter att förebygga brott.[35] Med tiden har lokalt brottsförebyggande arbete blivit ett begrepp.[36] (Se kapitel 2 i denna utredning.) Regeringen satsar nu ytterligare genom nationell samordning för att stödja kommunerna att förebygga brott.[37] Utredningen *En nationell samordnare för att värna demokratin mot våldsbejakande extremism* (SOU 2016:92)[38] drar mot den bakgrunden slutsatsen att det ligger ett *allmänintresse* (enligt kommunallagen) i att förebygga viss brottslighet; framför allt brott som direkt eller indirekt påverkar det stora flertalet. Att förebygga sådan brottslighet skulle således vara inom ramen för den kommunala kompetensen och ligga i kommunens intresse att förebygga, men utgör således ingen skyldighet för kommunen att agera. I detta ligger också att kommunmedlemmarnas fri- och rättigheter ska upprätthållas av kommunerna.

Samtidigt finns en gräns mot Polismyndighetens ansvar och de åtgärder som kommunen kan vidta. I praktiken blir det en fråga om *hur* kommunen förebygger brott, där det allmänna intresset knappast gäller sådana åtgärder som är förbehållna Polismyndigheten.

Att kommunen inte har något mer allmänt definierat ansvar för att förebygga brott stöds också av att det i vissa författningar uttryckligen föreskrivs ett ansvar, eller att ett sådant indirekt framgår till följd av kommunens kontroll- och tillsynsansvar. Således följer det av 5 kap. 11 § socialtjänstlagen (2001:453) att socialnämnden ska verka för att den som utsatts för brott och dennes närstående får stöd och hjälp. Socialnämnden ska särskilt beakta att kvinnor som är eller har varit utsatta för våld eller andra övergrepp av närstående kan vara i behov av stöd och hjälp för att förändra sin situation. Socialnämnden ansvarar för att ett barn, som utsatts för brott, och ett sådant barns närstående får det stöd och den hjälp som de

[34] Dalman m.fl., Kommunallagen med kommentarer och praxis, 5 uppl., 2011, s. 58.
[35] Ds 1996:59.
[36] Brå, Samverkan i brottsförebyggande arbete, 2016.
[37] Prop. 2016/17:1 s. 48.
[38] SOU 2016:92 s. 74.

behöver. Socialnämnden ska också särskilt beakta att ett barn som har bevittnat våld eller andra övergrepp av eller mot närstående är offer för brott, och ansvara för att barnet får det stöd och den hjälp som barnet behöver. Den 1 juli 2007 skärptes lagen så att socialnämndens skyldighet att ge brottsoffer stöd och hjälp framgår tydligare.[39]

Kommunen har också ett ansvar för olika ekobrott, vilket kan knytas till kommunens åliggande att pröva serveringstillstånd, genomföra miljötillsyn eller att utöva tobakskontroll.[40] Kommunen har också ett ansvar för att hantera extraordinära händelser enligt lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Det kan gälla krisberedskapen före, under och efter en allvarlig händelse, vilket kan involvera extremistiskt våld. Kommunen ska ha en plan för att hantera extraordinära händelser och bland annat kunna akut bistå med psykiskt och socialt omhändertagande (POSOM). Ansvaret gäller då inte själva brottsligheten (av extraordinär natur) utan beredskapen inför samt effekterna och följderna av den. Den kommunala krisberedskapen går mer och mer mot att omfatta även sociala risker.[41]

På missbruksområdet kan kommuner bl.a. besluta om omhändertagande enligt lagen (1990:52) med särskilda bestämmelser om vård av unga, förkortad LVU, respektive lagen (1988:870) om vård av missbrukare i vissa fall, förkortad LVM, fältassistenter, vårdplatser (LVU/LVM) och riktade informationsinsatser (t.ex. i skola) m.m.

Ett annat exempel är trygghet på allmän plats och målet att minska de faktorer som skapar otrygghet på allmän plats. För kommunernas del uppmärksammas bl.a. belysning, röjning av parkvägar, buskar m.m., klottersanering, lokala ordningsföreskrifter, trygghetsvandringar, extern och intern information och kameraövervakning på offentlig plats.

Samverkansöverenskommelser mellan polisen och kommuner berörs i kapitel 2. Ungdomar och ungdomsbrott är de områden som oftast är prioriterade i samverkansöverenskommelser. Vanligaste åtgärder är informationsinsatser samt alkohol- och narkotikaförebyggande åtgärder.

Det förekommer även samarbete i form av s.k. sociala insatsgrupper, där socialtjänsten har en viktig roll. Polisen, skolan och andra myndigheter kan föreslå individer som är lämpliga för arbetsmetoden genom att notera det på anmälningar till socialnämnden enligt 14 kap. 1 § socialtjänstlagen. Polisen kan även föreslå individer i samband med att information förs över till socialtjänsten i enlighet med 6 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare. Nämnas kan att för de individer som blir aktuella tas en åtgärdsplan fram, där det ska framgå vilka åtgärder som ska vidtas, vem som ska göra vad, när varje åtgärd ska vara slutförd och hur processen ska dokumenteras. Det är också viktigt att fastställa ordningen mellan åtgärderna. De åtgärder som vidtas för den unge ska följas upp av den sociala

[39] Prop. 2006/07:38, bet. 2006/07: SoU10, rskr. 2006/07:145.
[40] Brå 2015:15.
[41] SOU 2016:92 s. 75.

insatsgruppen. (Se broschyren Sociala insatsgrupper – vad är det, på polisens webb-plats.)

Lokala brottsförebyggande råd, som drivs av kommunerna, är i dag inrättade i nästan hela landet. Aktörer som polis, kriminalvård, skola, socialtjänst och näringsliv samarbetar för att förebygga brott och öka tryggheten.

Sammanfattningsvis är det inom ramen för den kommunala kompetensen i kommunallagen som kommunen kan och får engagerar sig i frågor om att förebygga viss brottslighet. Motioner har väckts om att kommunernas brottsförebyggande arbete ska tydliggöras i lag. De har hittills avslagits av Konstitutionsutskottet.[42]

2017 lanserade regeringen ett nytt brottsförebyggande nationellt program – *Tillsammans mot brott*. Programmet finns beskrivet i kapitel 3. I regeringens brottsförebyggande program är kommunerna en nyckelaktör i det brottsförebyggande arbetet, förutom flera statliga myndigheter utanför rättsväsendet. I programmet uppmärksammar regeringen även näringslivets roll. Civila samhällets kunskap och erfarenhet ska tas tillvara i högre utsträckning.

Mångfalden av aktörer och behovet av nära samarbete mellan offentlig sektor och näringsliv för att förebygga brott och få ned antalet brott i samhället ger vid handen att regeringen anser – genom det nationella programmet – att ett framgångsrikt arbete med programmet kräver att hela samhället sluter upp bakom detsamma. Det finns således helt klart ett samhällsintresse för att förebygga brott eftersom det berör alla och innebär stora kostnader för samhället och i många fall stort lidande för brottsoffer, både fysiskt och ekonomiskt.

Övervägande skäl talar således för att den rättsliga grunden för behandling av personuppgifter i Embrace, i de fall sådana uppgifter förekommer i tjänsten, står att finna i art. 6.1 e – utförande av ”arbetsuppgifter av allmänt intresse”. Det innebär bl.a. att de registrerade inte kan kräva att deras uppgifter i Embrace ska raderas.

Enligt dataskyddsförordningen måste dock en rättslig förpliktelse, myndighetsutövning eller arbetsuppgift av allmänt intresse vara fastställd i enlighet med nationell rätt eller unionsrätt för att kunna utgöra rättslig grund för behandling av personuppgifter. Som redovisas i avsnitt 7.3 förtydligas dessa företeelser i svensk rätt i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Beträffande den rättsliga grunden arbetsuppgifter av allmänt intresse så ska sådana uppgifter vara fastställda i enlighet med svensk rätt om de följer av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning (2 kap. 4 §).

Som konstaterats har inte kommunerna en uttrycklig skyldighet att bedriva brottsförebyggande arbete. Kommunens möjligheter att agera och vidta brottsförebyggande åtgärder framgår indirekt av kommunallagen och andra specialförfattningar. Det finns således härigenom stöd i författning för kommunerna behandling av personuppgifter i Embrace. Kommunerna kan således åberopa den rättsliga grunden i art. 6.1 e dataskyddsförordningen respektive 2 kap. 2 § 1 punkten i

[42] Se t.ex. Konstitutionsutskottets betänkande 2014/15: KU18.

dataskyddslagen för sin personuppgiftsbehandling i Embrace, dvs. att behandlingen är nödvändig för att utföra en arbetsuppgift av allmänt intresse.

Denna rättsliga grund kan dock inte åberopas av aktörer inom näringslivet när de behandlar personuppgifter i Embrace. För deras del blir det aktuellt att i stället åberopa den rättsliga grunden ”intresseavvägning” enligt art. 6.1. f dataskyddsförordningen (se avsnitt 8.6.3).

Utgångspunkten för bedömningen ovan är att en nämnd samlar in uppgifter direkt i sin egen instans av Embrace. Det är en personuppgiftsbehandling baserad enbart på dataskyddsförordningen och dataskyddslagen för ändamålet brottsförebyggande lokalt arbete, där kommunerna spelar en viktig roll.

Denna laglighetsprövning har inte beaktat import eller överföring av personuppgifter från kommunens olika förvaltningssystem. Inom vård och omsorg regleras personuppgiftsbehandlingen av patientdatalagen (2008:355) och lagen (2001:454) om behandling av personuppgifter inom socialtjänsten som kompletteras av en förordning. Överföring eller import av personuppgifter från vårdsystem eller socialtjänstsystem måste prövas med utgångspunkt från dessa registerlagar. Beträffande endast Polismyndigheten har en sådan laglighetsprövning genomförts, se avsnitt 8.6.2.

Eftersom det inte ska förekomma känsliga personuppgifter i Embrace, berörs inte behovet av rättslig grund för känsliga personuppgifter. Det bör dock erinras här att i fritextrutorna så öppnar Embrace upp för registrering av sådana uppgifter. Ett alternativ är att ta bort fritextrutorna helt och hållet. Ett annat alternativ är att det finns mekanismer i Embrace som förhindrar sådan registrering.

Dataskyddsförordningen ställer krav på inbyggt dataskydd (privacy by design) och dataskydd som standard (privacy by default) vid all slags hantering av personuppgifter (art. 25.1 och 25.2). Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas (inbyggt dataskydd).

Den personuppgiftsansvarige ska vidare genomföra lämpliga tekniska och organisatoriska åtgärder för att, i *standardfallet*, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer (dataskydd som standard).

En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven på inbyggt dataskydd och dataskydd som standard följs (art. 25.3).

Embrace är inte designat för att registrera enskilda individuppgifter. I nuläget finns – såvitt kan bedöms – godtagbara tekniska och administrativa funktioner på plats i Embrace som ska förhindra att individuppgifter och känsliga personuppgifter förekommer hos de enskilda användarna (personuppgiftsansvariga) eller lämnas ut av dem till den gemensamma lokala problembilden (se avsnitt 2.2). Det får betraktas som exempel på tekniska och administrativa åtgärder i enlighet med kraven på inbyggt dataskydd resp. dataskydd som standard i dataskyddsförordningen.

8.6.2 Rättslig grund för Polismyndigheten

Polisen är en brottsbekämpande myndighet vars personuppgiftsbehandling träffas av brottsdatalagen. Lagen är ett genomförande av brottsdatadirektivet i Sverige. Den lagen kompletteras i sin tur av specialförfattningar inom rättskedjan, såsom exempelvis polisdatalagen.

Polisen ska således iaktta polisdatalagens bestämmelser när den behandlar personuppgifter i Embrace, i nu föreliggande fall för brottsförebyggande syften. Polisens rättsliga grund för att behandla personuppgifter i Embrace finns således i den lagen. Polismyndigheten är personuppgiftsansvarig för behandlingen.

Polisdatalagen har varit föremål för översyn av Brottsdatautredningen (SOU 2017:29) och ett förslag till ny lag, lagen om polisens behandling av personuppgifter inom brottsdatalagens område, har presenterats riksdagen av regeringen (prop. 2017/18:269). Lagen träder i kraft den 1 januari 2019.

Även här finns anledning att uppmärksamma att Embrace inte är avsett att registrera känsliga personuppgifter. I denna del hänvisas till avsnitt 8.6.1. och dataskyddsförordningens krav på inbyggt dataskydd (privacy by design) och dataskydd som standard (privacy by default).

En fråga är om polisen har laglig rätt att behandla personuppgifter i Embrace. En annan om polisen får lämna ut uppgifter i Embrace till den gemensamma, lokala problembilden i Embrace Insight, där ett flertal olika mottagare kan ta del av uppgifterna, t.ex. kommuner samt bostads- och fastighetsbolag. Eftersom polisen i många fall är beroende av samverkan med andra, icke rättsvårdande myndigheter faller det sig naturligt att utbyta uppgifter med dessa. Men får polisen dessutom lämna ut uppgifter till privata aktörer som medverkar i det brottsförebyggande lokala samarbetet, t.ex. bussbolag eller bostads- och fastighetsbolag?

Myndighetssamverkan förutsätter utbyte av information. Ofta är det tillräckligt med avidentifierade uppgifter men i den operativa verksamheten kan det vara nödvändigt att utbyta information som innehåller personuppgifter. Det kanske finns betänkligheter från integritetsskyddssynpunkt att polisen lämnar ut personuppgifter från den brottsbekämpande verksamheten till andra myndigheter än de som har till uppgift att bekämpa brott.

En central del i det lokala samverkande arbetet mot brott och andra otrygga händelser är att alla parter delar och kompletterar varandras information (om brottsrelaterade och andra otrygghetsskapande händelser) i en så kallad gemensam lokal problembild. Det gäller inte bara kommuner och medverkande privata aktörer, t.ex. fastighets- och bostadsbolag, utan även polisen. Embrace innehåller således en sådan lokal problembild (Embrace Insight) där lokalt samverkande parter kan dela med sig (röja) sin information, och ta del av den.

Begreppet samverkan kan omfatta flera olika former av samarbete. Samverkan kan avse såväl diskussioner i strategiska frågor som mer operativt samarbete, t.ex. en planerad gemensam aktion. Ett exempel på samverkan som regeringen nämner är samverkan mellan polisen, Tullverket, Kustbevakningen och Migrationsverket vid gränskontroll.

Av polisdatalagen framgår således att personuppgifter som behandlas med stöd av 7 § för bl.a. brottsförebyggande syften får även behandlas när det är nödvändigt för att tillhandahålla information som behövs i t.ex. en myndighets verksamhet ”om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott” (2 kp. 8 § 1 stycket 7 b). Som exempel på en sådan myndighet kan nämnas en nämnd i en kommun som finns representerad i det lokala brottsförebyggande rådet, t.ex. en socialnämnd eller samhällsbyggnadsnämnd.

En särskild fråga är om polisen får lämna ut uppgifter i Embrace till andra aktörer än myndigheter i det brottsförebyggande arbetet, t.ex. näringslivet. Här avses den gemensamma, lokala problembilden i Embrace som alla lokalt samverkande parter har tillgång till och ”föder” med information om brottsrelaterade och andra otrygghetsskapande händelser.

Polisdatalagen reglerar i huvudsak enbart behandling av personuppgifter för tillhandahållande av information till myndigheter. Undantagsvis får polisen enligt lagen lämna ut personuppgifter i en förundersökning till en konkursförvaltare, oftast en advokat (2 kap. 8 § 3 stycket). Några andra privaträttsliga subjekt nämns inte uttryckligen i lagen, t.ex. fastighets- och bostadsföretag eller bussföretag. Inte heller lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet innehåller några bestämmelser om utlämnande av polisiära uppgifter till privata aktörer.

Det behöver inte utgöra ett problem för polisen att dela med sig av information i den gemensamma problembilden i Embrace. Flertalet uppgifter i Embrace utgör ju inte personuppgifter i personuppgiftslagens mening. De kan varken direkt eller indirekt hänföras till en fysisk levande person. Polisdatalagen (brottsdatalagen) är därmed inte tillämplig på sådana uppgifter, och polisen kan fritt behandla dessa och dela med sig av dem till andra mottagare än myndigheter.

Som konstaterats kan dock gatu- och adressuppgifter i Embrace indirekt hänföras till fysiska personer som är i livet. Det rör sig då om personuppgifter, om namn och personnummer saknas.

I 2 kap. 8 § polisdatalagen regleras som nämnts tämligen detaljerat till vilka aktörer polisen får lämna ut personuppgifter för de ändamål som räknas upp i 7 §,

bl.a. brottsförebyggande arbete. Några privata aktörer finns, som sagt, inte upptagna. Uppräkningen av mottagare i bestämmelsen är dock inte uttömmande.

I ett enskilt fall får personuppgifter som polisen samlat in för t.ex. brottsförebyggande arbete även behandlas för att tillhandahålla information för något annat ändamål än de som anges i 2 kap. 8 § 2 – 3 styckena i lagen, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in. Det framgår av fjärde stycket i 2 kap. 8 § polisdatalagen. Bestämmelsen är ett uttryck för den s.k. *finalitetsprincipen*.

Finalitetsprincipen är ett grundläggande krav i personuppgiftslagen om att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (se 9 § punkten d) personuppgiftslagen). I en sådan bedömning får man hypotetiskt utgå från hur en registrerad typiskt sett (inte den registrerade i det enskilda fallet) skulle se på saken. Kommer man i en sådan bedömning fram till att den registrerade rimligen har att räkna med att de insamlade personuppgifterna också får behandlas för det nya ändamålet, kan det nya ändamålet inte anses vara oförenligt med det ursprungliga ändamålet.

Ändamålen i paragrafen är alltså inte uttömmande. För att en uppgift ska få vidarebehandlas för något annat ändamål än de som anges i första–tredje styckena måste det emellertid i det enskilda fallet göras en bedömning att det nya ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in, en s.k. oförenlighetsprövning.

I Embrace fall är ändamålet brottsförebyggande arbete. Det är inte ett ändamål som är oförenligt med polisens egen insamling av uppgifter, t.ex. genom brottsanmälningar. Vissa uppgifter ur dessa anmälningar är av betydelse för polisens brottsförebyggande arbete och samverkan på lokal nivå. De kan således importeras av polisen från det system där brottsanmälningar (RAR) finns till polisens egen instans av Embrace och sedan delas med andra aktörer i det lokala brottsförebyggande arbetet.

Ett utlämnande av eventuella personuppgifter till den gemensamma problembilden i molntjänsten, som är åtkomlig för andra behöriga aktörer, t.ex. fastighets- och bostadsföretag, bedöms utgöra en tillåten behandling enligt polisdatalagen. Ett utlämnande bedöms inte heller vara oförenlig med offentlighets- och sekretesslagen i de fall uppgifterna indirekt kan hänföras till en fysisk levande person (se avsnitt 8.7). Det erinras att det är Polismyndigheten som ska göra denna oförenlighetsprövning.

Av bestämmelsen framgår dock att behandling av personuppgifter för sekundära ändamål är tillåtet under förutsättning att det i ett ”enskilt fall” inte kan anses oförenligt med insamlingsändamålet att lämna ut uppgifterna. Det är något oklart vad som avses med det begreppet. Paralleller kan dras till sekretesslagstiftningen. Som regel ska en myndighet göra en konkret och individuell prövning av ett utlämnande, uppgift för uppgift. Ibland kan emellertid en sådan procedur vara praktiskt ogenomförbar. Myndigheten, till exempel en nämnd i ett landsting som ansvarar för hälso- och sjukvård, kan helt enkelt inte bilda sig en rimlig uppfattning om den

särskilda skaderisk som kan vara förbunden med varje enskild uppgift som kontinuerligt tillförs patientens journal.

I sådana situationer får i stället en myndighet göra en schabloniserad menprövning, i analogi med vad som i förarbetena till sekretesslagen förordas vid så kallat massuttag.[43] De kunskaper som myndigheten har om mottagaren eller mottagarna, hur dessa kommer att hantera uppgifterna och vilken risk för ytterligare spridning som finns, kan då – tillsammans med en bedömning av den skaderisk som typiskt sett är förbunden med uppgifter av aktuellt slag – i de allra flesta fall ge fullt tillräckligt underlag för bedömningen av om sekretessbestämmelsens skaderekvisit är uppfyllt och sekretess därmed gäller eller inte gäller gentemot mottagaren i fråga.

På motsvarande sätt kan Polismyndigheten göra en schabloniserad oförenlighetsprövning för Embrace Insight (den gemensamma problembilden som alla lokalt samverkande parter i det lokala brottsförebyggande rådet har tillgång till) med utgångspunkt från de uppgifter som typiskt utgör personuppgifter, främst gatu- och fastighetsadresser, och i samband med det också göra en schabloniserad menprövning, vilken prövning bör dokumenteras och sedan läggas till grund för ett beslut av Polismyndigheten om upprepade utlämnanden av personuppgifter med koppling till gatu- och fastighetsadresser till den gemensamma problembilden. Sekretessfrågorna behandlas nedan.

Som framhållits är många uppgifter i Embrace inte personuppgifter. Personuppgifter kan uppstå om händelser eller insatser kan hänföras till en gatu- och bostadsadress som indirekt kan kopplas till de fysiska personer som bor på adressen eller i fastigheten. I de fallen bedöms en utlämnandebehandling med avseende på den gemensamma problembilden inte vara oförenliga med polisdatalagens primära insamlingsändamål och därför kunna lämnas ut med stöd av 2 kap. 8 § fjärde stycket till privata aktörer, t.ex. bostads- och fastighetsbolag.

Enligt 2 kap. 20 § får polisen lämna ut enstaka personuppgifter på medium för automatiserad behandling (ADB-utlämnande). ADB-utlämnande saknar en legaldefinition. Utlämnandeformen innebär ett elektroniskt utlämnande utan möjlighet för mottagaren att själv bereda sig tillgång till uppgifterna, t.ex. genom användning av e-post, utlämnande på ett lagringsmedium (DVD, USB) eller genom filöverföring från ett informationssystem till ett annat. Enligt paragrafen får regeringen meddela föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall. I polisdataförordningen har regeringen bl.a. föreskrivit att polisen får ADB-utlämna uppgifter till bl.a. målsägandebiträde och offentlig försvarar i större utsträckning än ”enstaka personuppgifter”. Några andra privata aktörer finns inte nämnda.

Av 21 § i samma kapitel framgå att utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av denna lag. Begreppet direktåtkomst används i dag i olika registerförfattningar med något varierande innebörd. Direktåtkomst saknar en legaldefinition. Direktåtkomst är en form av elektroniskt utlämnande av personuppgifter. Enligt olika förarbeten innebär direktåtkomst att den som är

[43] Prop. 1979/80:2 Del A s. 80 f.

ansvarig för informationen inte har kontroll över vilka uppgifter som en behörig mottagare vid ett visst tillfälle tar del av, och att mottagaren av informationen inte kan påverka innehållet i det informationssystem som informationen lämnas ut från. Inom offentlig verksamhet aktualiseras direktåtkomst främst vid utlämnande över myndighetsgränser. I princip tillåter polisdatalagen enbart direktåtkomst för myndigheter, inte privata aktörer.

Polisens utlämnande av eventuella personuppgifter till Embrace Insight (den gemensamma problembilden) ska således ske genom ADB-utlämnande, inte genom direktåtkomst. Genom utlämnandet blir uppgifterna tillgängliga för andra mottagare, tillika aktörer i det lokala brottsförebyggande arbetet. Såvitt förstås är det också på det sättet uppgifter lämnas ut. Varje aktör som använder Embrace ska utse en administratör som säkerställer att inte individ- eller sekretessbelagda uppgifter lämnas till Embrace Insight. Man skulle kunna önska sig en tydligare utlämnandebestämmelse i polisdatalagen som tillåter polisen att lämna ut uppgifter till privata aktörer som medverkar i det lokala brottsförebyggande arbetet. Särskilt med tanke på att uppgifter i Embrace kan utgöra personuppgifter. Sådana uppgifter kan förekomma i Embrace när en händelse eller insats kopplas till en specifik gatu- eller bostadsadress där det finns hyresgäster eller andra boende fysiska personer. Det finns därför anledning att väcka frågan om en kompletterande bestämmelse i den nya lagen om polisens behandling av personuppgifter inom brottsdatalagens område som träder i kraft 1 januari 2019 eller i kompletterande ny förordning om polisens behandling av personuppgifter inom brottsdatalagens område som tydligare medger utlämnandebehandling till privata aktörer som medverkar i det gemensamma lokala brottsförebyggande arbetet, inte minst mot bakgrund av regeringens nationella brottsförebyggande program – *Tillsammans mot brott* (2017), vari näringslivet spelar en viktig roll i det arbetet.

Eftersom det inte ska förekomma känsliga personuppgifter i Embrace, berörs inte behovet av laglig grund för känsliga personuppgifter inom polisen. Beträffande känsliga personuppgifter samt kraven på inbyggt dataskydd och dataskydd som standard enligt brottsdatalagen hänvisas till redogörelsen i avsnitt 8.6.1.

8.6.3 Laglig grund för aktörer inom näringslivet m.fl.

Användare inom näringslivet, bostads- och fastighetsföretag och andra aktörer inom näringslivet som samarbetar med varandra för att förebygga brott, bedöms lagligen kunna behandla personuppgifter i Embrace efter en *intresseavvägning* (se 10 § f PUL samt art. 6.1 f dataskyddsförordningen). Artikeln lyder som följer:

”Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.”

Det är således en avvägning mellan olika intressen som ska läggas till grund för personuppgiftsbehandlingen, varvid intresset av att behandla personuppgifter är

berättigat i jämförelse med skyddet för den personliga integriteten. Bostads- och fastighetsföretag får anses helt klart höra till den kategori av aktörer som har ett berättigat intresse av att behandla personuppgifter i Embrace med hänsyn till deras påverkansmöjligheter för en trygghetsskapande miljö, varvid intresset för att skydda enskildas personliga integritet får ge vika. I regeringens nationella brottsförebyggande program, Tillsammans mot brott (2017), framhålls bostadspolitiken som ett prioriterat område för det brottsförebyggande arbetet.[44]

Någon sannolik hög risk för enskildas fri och rättigheter bedöms inte föreligga med hänsyn till att Embrace inte hanterar individuppgifter utan bara i vissa fall uppgifter (gatu- och fastighetsadresser) som indirekt kan hänföras till en eller flera individer. Med stöd av den rättsliga grunden ”intresseavvägning” behöver t.ex. ett fastighets- eller bostadsföretag inte inhämta ett samtycke för sin registrering av uppgifter i Embrace, såvida det rör sig om personuppgifter i förordningens mening.

Vad som nu sagt om den rättsliga grunden för bostads- och fastighetsbolag innebär inte med automatik att andra aktörer, t.ex. bussbolag, eller motsvarande som vill arbeta brottsförebyggande kan åberopa samma grund. Övervägande skäl talar för det, men en laglighetsprövning ska göras av varje organisation själv som vill använda Embrace, se avsnitt 8.4.

Kommunala bostads- och fastighetsbolag utgör inte myndigheter i dataskyddsförordningens eller dataskyddslagens mening. Dessa bolag står dock under en kommunal styrning. Regeringen anför att de uppgifter av allmänt intresse som utförs i syfte att utföra ett uttryckligt uppdrag eller till följd av ett åliggande, måste anses vara av allmänt intresse oavsett om de faktiskt utförs i myndighetens egen regi, av egna anställda, eller om de genom utkontraktering utförs av någon annan. När en juridisk eller fysisk person, på uppdrag av en kommunal eller statlig myndighet, utför en förvaltningsuppgift som åligger kommunen eller myndigheten, bör alltså enligt utredningen även den privata utföraren, entreprenören eller det kommunala bolaget anses utföra en uppgift av allmänt intresse.[45] Som exempel på sådana uppgifter av allmänt intresse som kommunerna utför på frivillig grund nämner regeringen ”tillhandahållande av bostäder”.[46]

Sammanfattningsvis utgör kommunala bostads- och fastighetsbolag inte myndigheter i lagens mening, men kan åberopa samma lagliga grund som kommunen, dvs. utförande av ”arbetsuppgifter av allmänt intresse” (6.1 e samt 2 kap. 4 § i dataskyddsförordningen) eftersom dessa bolag lyder under kommunal styrning och tillhandahållande av bostäder är av allmänt intresse.

Eftersom det inte ska förekomma känsliga personuppgifter i Embrace, berörs inte behovet av laglig grund för känsliga personuppgifter för de privata aktörerna. Beträffande känsliga personuppgifter samt kraven på inbyggt dataskydd och dataskydd som standard enligt dataskyddsförordningen hänvisas till redogörelsen i avsnitt 8.6.1.

---

[44] Skr. 2016/17:126 s. 4.
[45] Prop. 2017/18:105 s. 58.
[46] Ib. s. 57.

8.7 Sekretessfrågor m.m.

Bedömning: För flertalet uppgifter i kommunens egen instans av Embrace råder ingen sekretess eftersom de inte kan hänföras till någon individ utan enbart till en plats. Sådana uppgifter kan utan risk för men eller skada för enskilda fysiska personer göras tillgängliga i den gemensamma, lokala problembilden i Embrace (Embrace Insight), t.ex. för Polismyndigheten samt bostads- och fastighetsbolag.

Sekretess kan aktualiseras avseende händelser kopplade till adress- och fastighetsuppgifter i Embrace, vilka kan indirekt hänföras till enskilda individer som bor på adressen. Även här bedöms risken som liten för men eller skada för enskilda fysiska personer, och uppgifterna borde kunna lämnas ut utan hinder av sekretess. Det är emellertid varje nämnds ansvar att beakta tillämpliga sekretessbestämmelser.

Beträffande Polismyndigheten görs samma bedömning. Vissa uppgifter i Embrace utgör inte personuppgifter och kan riskfritt lämnas ut av polisen till den gemensamma lokala problembilden i Embrace (Embrace Insight). Utlämnande kan i tveksamma fall, främst beträffande händelser i polisens instans i Embrace som är kopplade till gatu- och fastighetsadresser till bostadshus, ske inom ramen för antingen ett nödvändigt utlämnande (10 kap. 2 § offentlighets- och sekretesslagen) eller en intresseavvägning med stöd av den s.k. generalklausulen i 10 kap. 27 § i samma lag, oavsett om mottagaren är en icke brottsbekämpande myndighet eller privat aktör, vilka samverkar med polisen på lokal nivå.

Det erinras att en myndighets uppgifter i Embrace Insight kan anses inkommen, och därmed utgöra en förvarad allmän handling hos en annan myndighet som har en teknisk åtkomst till Embrace Insight (2 kap. 3 § tryckfrihetsförordningen). Allmänheten och media kan därmed vända sig till vem som helst av myndigheterna och begära ut uppgifter ur Embrace Insight. Myndigheten som har att ta ställning till en sådan begäran ska i sådant fall göra en menprövning i sedvanlig ordning.

Privata aktörer bestämmer själva vilken information i Embrace de vill dela med t.ex. polisen eller kommunen. Kommunala bostads- och fastighetsbolag ska dock, liksom kommuner, beakta offentlighets- och sekretesslagens bestämmelser, när de lämnar ut uppgifter till någon utanför organisationen. Enligt den lagen är bolagen att likställa med myndigheter.

I föreliggande avsnitt behandlas sekretessfrågor. Sekretess och tystnadsplikt regleras i dels offentlighets- och sekretesslagen, dels i andra specialförfattningar. En orientering på området finns i avsnitt 4.8.

En myndighet ska alltid iaktta sekretess och tystnadspliktsbestämmelser när den överväger att lämna ut en allmän handling till en mottagare utanför myndigheten, antingen på begäran av enskild person med stöd av tryckfrihetsförordningens bestämmelser om utfående av allmänna handlingar, på begäran av en annan myndighet eller självmant till någon av dessa mottagare. Handlingen kan visa sig vara offentlig, och kan lämnas ut, eller så råder sekretess för uppgiften. I det senare

fallet är myndigheten förhindrad att lämna ut en allmän handling till en mottagare. Ibland kan uppgiften omfattas av sekretess även hos en mottagande myndighet. Det kan underlätta utlämnande av en hemlig uppgift som annars inte skulle kunna lämnas ut. I andra fall kan en myndighets sekretess så att säga följa med uppgiften och mottagande myndighet kan då åberopa samma sekretess som utlämnande myndighet. Även det underlättar ett utlämnande av en hemlig uppgift till mottagaren.

Sekretess innebär ett förbud mot att ”röja” en uppgift, oavsett om det görs muntligen, genom utlämnande av allmän handling eller på något annat sätt (3 kap. 1 § OSL). Röja” kan översättas med att låta någon ta del av en uppgift, oavsett om mottagaren faktiskt har tagit eller kommer att ta del av uppgiften. Det spelar inte någon roll om mottagaren faktiskt har tagit eller kommer att ta del av uppgiften. Det väsentliga är i stället själva tillåtandet eller tillgängliggörandet. Som exempel kan nämnas att den som skickar ett vanligt brev eller ett e-postmeddelande innehållande sekretessbelagda uppgifter till en utomstående, obehörig person får anses ha röjt dessa uppgifter, även om mottagaren ännu inte har öppnat brevet eller meddelandet och tagit del av innehållet.

Detta innebär att även om det som regel räcker att en hemlig uppgift har gjorts tillgänglig för någon obehörig, ska det inte betraktas som ett röjande om tillgängliggörandet har skett på ett sådant sätt att det kan antas att mottagaren inte kommer att ta del av uppgiften. I vart fall när sekretessbelagda uppgifter tillgängliggörs under sådana omständigheter att det förefaller osannolikt att mottagaren tar del av uppgifterna kan ett röjande i OSL:s mening inte anses ha ägt rum.[47] Så är oftast fallet vid en myndighets outsourcing av sekretessbelagda uppgifter till en leverantör för enbart teknisk bearbetning eller teknisk lagring av uppgifterna. Uppgifterna är inte nödvändigtvis röjda i en sådan situation.

I Embrace lämnar bl.a. myndigheter ut uppgifter till den gemensamma problembilden i (Embrace Insight) där andra behöriga myndigheter eller privata aktörer som använder Embrace kan ta del av de utlämnade uppgifterna inom ramen för ett gemensamt, lokalt brottsförebyggande arbete. Här är således syftet med själva tillgängliggörandet att andra samverkande aktörer ska få ta del av de utlämnade uppgifterna om brottsrelaterade och andra otrygghetsskapande händelser. Det innebär att en myndighets utlämnade uppgifter är ”röjda”. Därmed inte sagt att det rör sig om ”röjda” hemliga uppgifter. Det avgör myndigheten med hänsyn till typen av uppgifter och vilka mottagarna är.

I Embrace finns inga individuppgifter, och risken för att enskilda ska drabbas av men eller skada är väldigt liten om en myndighet lämnar ut sådana uppgifter till den gemensamma problembilden (Embrace Insight). Mekanismer finns vidare på plats hos varje aktör för att hindra att uppgifter som skulle kunna innebär men eller skada för en fysisk person eller för en brottsutredning lämnas ut till den gemensamma problembilden. Syftet är att alla delaktiga aktörer, t.ex. Polismyndigheten, kommunen och bostads- och fastighetsbolag m.fl. privata aktörer i det

[47] eSam, Outsourcing – en vägledning om sekretess och persondataskydd, 2016, s. 16 f.

brottsförebyggande arbetet ska kunna arbeta med uppgifterna i den gemensamma problembilden.

Vem som helst kan inte ta del av uppgifterna i den gemensamma problembilden (Embrace Insight) utan de finns alltjämt i en sluten miljö, där både myndigheter och privata aktörer kan dela information. Det skulle tala för ett visst mått av utrymme att röja uppgifter som är delvis eller helt hemliga i den gemensamma problembilden.

En myndighet bör dock ta i beaktande att man genom tillgängliggörandet av uppgifter om brottsrelaterade och andra otrygghetsskapande händelser inte längre utövar kontroll över ”röjda” uppgifter i Embrace Insight. Många aktörer, inte enbart myndigheter, kan vara delaktiga i det lokala, gemensamma brottsförebyggande arbetet. Varje myndighet som använder Embrace ska således ta i beaktande vid sin utlämnandeprövning att utlämnade uppgifter kan få en vidare spridning än den krets av användare som har direkt tillgång till Embrace Insight. Det kan t.ex. handla om en förvaltningsenhet inom en kommun eller ett bostadsbolag som samverkar i det lokala brottsförebyggande arbetet och genomför en presentation av den gemensamma problembilden för kommunens eller bostadsbolagets ledningsgrupp. Varje myndighet som använder Embrace ska vara medveten om vid sin utlämnandeprövning att de uppgifter man lämnar ut till Embrace Insight ska tåla en sådan spridning av uppgifter utan risk för men eller skada för enskild fysisk person eller en brottsutredning.

Det erinras också att en myndighets uppgifter i Embrace Insight kan anses inkommen, och därmed utgöra en förvarad allmän handling hos en annan myndighet som har en teknisk åtkomst till Embrace Insight (2 kap. 3 § tryckfrihetsförordningen). Allmänheten och media kan därmed vända sig till vem som helst av myndigheterna och begära ut uppgifter ur Embrace Insight. Myndigheten som har att ta ställning till en sådan begäran ska i sådant fall göra en menprövning i sedvanlig ordning. Som framhålls nedan bedöms inte de uppgifter som lämnas ut till Embrace Insight omfattas av sekretess eftersom de rör platser och inte enskilda individer. Det är inte uteslutet dock att en begäran om en sammanställning av uppgifter i Embrace Insight kan omfattas av sekretess. Det avgör den myndighet som får en sådan begäran, givet att det finns en tillämplig sekretessbestämmelse.

I de kommande avsnitten berörs utlämnande av uppgifter inom den kommunala sfären. Därefter berörs polisens möjligheter att lämna ut uppgifter till den gemensamma, lokala problembilden i Embrace. Och slutligen övervägs de privata aktörerna utlämnandefrågor.

8.7.1 *Kommuner*

Generellt torde sekretess sällan utgöra hinder för en kommunal förvaltning att lämna ut uppgifter eller röja uppgifter för andra mottagare i Embrace Insight (den gemensamma, lokala problembilden). Risken för men eller skada av något slag för enskilda fysiska personer torde vara liten eftersom Embrace inte innehåller individrelaterade uppgifter utan enbart platsuppgifter.

Beroende på vilken förvaltning som använder Embrace kan sekretess för uppgifterna i Embrace aktualiseras. Socialnämndens verksamhet omfattas för övrigt av en stark sekretess. Det finns också en generell sekretessbestämmelse för skydd av *personliga förhållanden* som kommunen kan åberopa, oavsett i vilket sammanhang uppgiften förekommer (21 kap. 1 § offentlighets- och sekretesslagen).

Huruvida det finns skäl att sekretessbelägga uppgifter i Embrace, och därmed inte lämna ut uppgifterna till den gemensamma problembilden i Embrace som andra aktörer, t.ex. polisen och privata aktörer, kan ta del av, får bedömas i det enskilda fallet av berörd nämnd.

Som nämnts innehåller Embrace inga individuppgifter. Icke förty kan gatu- och adressuppgifter kopplas till enskilda personer i hushåll på sådana adresser, och det kan inte uteslutas att sekretess kan aktualiseras för vissa sådana uppgifter som kan vara till men om de lämnas ut till den lokala gemensamma problembilden i Embrace Insight. Embrace registrera aldrig händelser som sker i en bostad. Men det går inte att utesluta kopplingen mellan adressen och den eller de personer som bor på adressen kan väcka frågor om sekretess, trots att händelsen inträffat utanför eller på fastigheten. Som exempel kan nämnas personer med skyddade personuppgifter (sekretessmarkering, kvarstad eller skyddad identitet) som bor på den specifika gatuadressen. Det kan också råda förundersökningssekretess för händelsen som är kopplad till en specifik gatuadress, och kommunens röjande av adressen skulle kunna försvåra polisens utredning. Det är lämpligt att i sådana fall kontakta polisen och få besked om en viss händelse vid en specifik gatu- eller fastighetsadress kan registreras. Det är sådana särskilda hänsynstaganden som kommuner och andra myndigheter som använder Embrace bör iaktta.

Det går inte att här redogöra för i vilka fall uppgifter kan tänkas omfattas av sekretess, och därmed inte kan lämnas ut till den gemensamma problembilden i Embrace. Det är varje myndighets ansvar att bedöma risken för men eller skada för enskilda fysiska personer med utgångspunkt från tillämpliga sekretessbestämmelser, och i slutändan är det den ansvariga nämnden som i varje enskilt fall av utlämnande ska avgöra vilka uppgifter i Embrace man vill lämna ut till Polismyndigheten och enskilda aktörer, t.ex. fastighets- och bostadsbolag.

Vid prövningen ska nämnden givetvis väga in om mottagaren omfattas av en författningsreglerad tystnadsplikt och sekretess för de uppgifter som nämnden delar med sig av i den gemensamma problembilden i Embrace. Polisen kan åberopa ett flertal sekretessbestämmelser om någon från allmänheten skulle vända sig till Polismyndigheten och begära ut uppgifter ur den gemensamma problembilden som en kommun bidragit med. Privata bostads- och fastighetsbolag, för att nämna ett exempel på aktör som använder Embrace, omfattas dock inte av en författningsreglerad sekretess eller tystnadsplikt. Nämnden måste därför ta privata aktörer i beaktande när man avser att lämna ut uppgifter till den gemensamma problembilden i Embrace.

Sammanfattningsvis torde sekretess sällan föreligga för uppgifter i Embrace eftersom tjänsten inte innehåller några individuppgifter. Det gäller även de fall där

sekretess kan aktualiseras beträffande händelser kopplade till adress- och fastighetsuppgifter i Embrace. Det är framför allt händelser kopplade till gatu- och fastighetsadresser där fysiska personer har sitt hushåll eller stadigvarande vistas som sekretess kan aktualiseras. Det är varje nämnds ansvar att beakta tillämpliga sekretessbestämmelser.

8.7.2 *Polismyndigheten*

Frågan om polisens möjligheter att dela brottsrelaterad information med andra myndigheter berördes av regeringen i propositionen till polisdatalagen[48]. Regeringen anförde att ett sådant uppgiftsutlämnande förekommit sedan länge, och att uppgifterna kunde lämnas ut av polisen med stöd av den s.k. generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen efter en intresseavvägning (se avsnitt 4.8.3). Regeringen ansåg att polisen behövde även fortsättningsvis ges möjlighet att behandla uppgifter för att tillhandahålla information till andra än brottsbekämpande myndigheter, när syftet är att samverka mot brott. Regeringen uppgav att information bör få tillhandahållas om utlämnandet kan vara till nytta för den brottsbekämpande verksamheten.

Embrace innehåller emellertid inga individuppgifter. Någon risk således att polisen åsamkar enskilda personer men eller skada genom att lämna ut uppgifter från sin egen instans av Embrace till den gemensamma problembilden bedöms som obefintlig.

Händelser som däremot är kopplade till specifika gatu- och adressuppgifter i Embrace kan kräva särskild uppmärksamhet i sekretesshänseende om uppgifterna kan kopplas till enskilda personer i hushåll på adressen. Som exempel har nämnts att individerna som bor på adressen har skyddade personuppgifter och därför till inget pris vill bli röjda. Det torde höra till undantagen. Många händelser och insatser i Embrace är bara kopplade till allmänna, publika platser, t.ex. torg, köpcentra och parker, och kan svårligen hänföras till enskilda fysiska personer, även om man registrerar gatuadress.

Även om sekretess kan råda för vissa händelser eller insatser kan polisen lämna ut uppgifterna med stöd av antingen generalklausulen i offentlighets- och sekretesslagen (se ovan), varvid en intresseavvägning ska göras mellan nyttan av att röja uppgifterna och risken för men eller om det är nödvändigt för att myndigheten ska kunna fullgöra sina arbetsuppgifter (10 kap. 2 § offentlighets- och sekretesslagen). Råder förundersökningssekretess för uppgifter ska de inte delas med andra lokalt samverkande parter.

Några hinder för polisen att lämna ut eller dela uppgifter i Embrace med enskilda representanter inom det lokala näringslivet, t.ex. bostads- och fastighetsbolag som aktivt medverkar i det lokala brottsförebyggande arbetet, bedöms inte föreligga, men det ska ske med beaktande alltid av gällande sekretessbestämmelser. Det är dock varje myndighets ansvar att bedöma risken för men eller skada för enskilda fysiska

[48] Prop. 2009/10:85.

personer, och i slutändan är det Polismyndigheten som ska avgöra vilka uppgifter myndigheten vill dela i Embrace med kommuner och enskilda aktörer, t.ex. fastighets- och bostadsbolag. Polismyndigheten äger också möjligheten att göra en schabloniserad menprövning enligt vad som framgår av avsnitt 8.6.2.

8.7.3 Privata aktörer

Privata aktörer bestämmer själva vilken information de vill dela med polisen eller kommunen. De omfattas inte av offentlighets- och sekretesslagens bestämmelser eller annan tystnadspliktsreglering. Kommunala bostads- och fastighetsbolag ska dock, liksom kommuner, beakta offentlighets- och sekretesslagens bestämmelser, när de lämnar ut uppgifter till någon utanför organisationen. Enligt den lagen är bolagen att likställa med myndigheter. Se avsnitt 8.7.1.

8.8 Förbudet för andra än myndigheter att behandla uppgifter om brott

Bedömning och rekommendationer: I Embrace registreras som regel händelser om vad, var, när och åtgärd. Bilder kan också registreras, men enbart med syfte att följa upp insatser på platser som är särskilt drabbade av brottsrelaterade och andra otrygghetsskapande händelser. Det kan röra sig om bilder på klotter eller annan skadegörelse samt förändringar i miljön som vidtagits för att undvika klotter.

Bilder och fotografier kan utgöra personuppgifter om man kan härleda dessa direkt eller indirekt till en fysisk levande person. Ibland kan en bild, t.ex. ett fotografi av klotter, röja vem som står bakom klottret. Klotter är en form av brottslig skadegörelse, och därmed uppstår en situation där personuppgifter behandlas om inte enbart en brottslig gärning utan dessutom en känd gärningsman. Enligt artikel 10 dataskyddsförordningen är det förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser. Förbudet för andra än myndigheter att behandla uppgifter om lagöverträdelser i artikel 10 i dataskyddsförordningen aktualiseras främst för de användare av Embrace som finns inom näringslivet, t.ex. bostads- och fastighetsbolag. Förbudet bedöms dock inte vara tillämpligt på majoriteten av uppgifter som registreras som text eller bild i Embrace av dessa privata aktörer. Skälet är att förbudet tar fasta på uppgifter om *den som begått ett brott och inte uppgifter om brottsoffer*. En bild på en krossad glasruta på en viss fastighet samt registrering av gatuadressen träffas i normalfallet således inte av förbudet i artikel 10 dataskyddsförordningen eftersom det inte rör sig om behandling av personuppgifter om lagöverträdelser.

Fotografier av klotter och annan skadegörelse av vilka framgår kännetecken för en viss gärningsmans arbetssätt, s.k. modus operandi, vid brott riskerar dock att träffas av förbudet i artikel 10.

Redan i dag har emellertid Embrace Safety AB utbildning samt tekniska och administrativa funktioner på plats i Embrace som ska förhindra att individuppgifter alternativt känsliga personuppgifter registreras i tjänsten. Utbildningen och

kontrollen bör även uppmärksamma att bilder på taggar på klotter och modus operandi som utvisar misstänkt gärningsman kan utgöra personuppgifter om lagöverträdelser. Sådana uppgifter får inte förekomma i Embrace om tjänsten används av privata aktörer inom näringslivet. Embrace Safety AB rekommenderas att friskriva sig från allt ansvar för dessa kunders registrering – eventuellt – av digitala bilder som utvisar vem som har begått ett brott.

Embrace Safety AB bör informera och utbilda kommuner och polisen om att de inte får dela bilder i Embrace Insight (den lokala gemensamma problembilden) med privata användare som utvisar vem som begått ett brott. En sådan delning kan vara straffbar. Även i detta fall rekommenderas Embrace Safety AB att implementera mekanismer i själva tjänsten som förhindrar sådan informationsöverföring till privata aktörer.

8.8.1 Inledning

Enligt Embrace Safety AB är fastighets- och bostadsföretag en målgrupp för tjänsten Embrace. Av regeringens nationella brottsförebyggande program – Tillsammans mot brott (2017) – spelar näringslivet en viktig roll i det lokala brottsförebyggande arbetet.

Det finns emellertid begränsningar för privatpersoner och företag att behandla personuppgifter i vissa avseenden. Det följer av artikel 10 dataskyddsförordningen. Enligt artikeln får behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet. Det rör sig således om personuppgifter om lagöverträdelser som innefattar brott, fällande domar i brottmål samt straffprocessuella tvångsmedel, t.ex. häktning, reseförbud och beslag.

Det är oklart om misstanke om brott ska räknas som personuppgifter om lagöverträdelser enligt artikel 10.[49]

Av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) framgår att personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning får behandlas av myndigheter (3 kap. 8 §).

Även andra än myndigheter får behandla sådana personuppgifter, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv. Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla sådana personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning (3 kap. 9 §). Den myndighet som regeringen bestämmer får i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter. Ett beslut får förenas med villkor.

[49] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/kansliga-personuppgifter/personuppgifter-som-ror-lagovertradelser/

Enligt 5 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning får personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning behandlas av andra än myndigheter om behandlingen är nödvändig för att

1. rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, eller
2. en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras.

Enligt 6 § får Datainspektionen meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning. Datainspektionen får även i enskilda fall besluta att andra än myndigheter får behandla sådana personuppgifter.

Frågan är således om fastighets- och bostadsföretag omfattas av detta förbud i artikel 10 i dataskyddsförordningen och om något av undantagen i dataskyddslagen och förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning är tillämpliga. Vidare frågas om förbudet i artikel 10 omfattar enbart uppgifter om förövaren, men inte uppgifter om brottsoffren?

Som konstaterats i avsnitt 8.6 får både kommuner och privata aktörer inom näringslivet, t.ex. bostads- och fastighetsbolag, lagligen behandla personuppgifter i Embrace, i de fall sådana uppgifter förekommer i tjänsten, förvisso med olika lagstöd. Kommunernas behandling av personuppgifter regleras av dataskyddsförordningen och dataskyddslagen, och den rättsliga grunden består i att det finns ett allmänt samhällsintresse av att kommuner är aktiva i det lokala brottsförebyggande arbetet samt i regeringens nationella brottsförebyggande program, där kommunerna spelar en nyckelroll (se avsnitt 8.6.1).

Fastighets- och bostadsföretagen, liksom sannolikt andra privata aktörer, får lagligen behandla personuppgifter, i de fall sådana uppgifter förekommer i Embrace, med stöd av den lagliga grunden ”intresseavvägning”, såvida de behandlar personuppgifter för lokalt brottsförebyggande arbete i samverkan med t.ex. kommunen och polisen (se avsnitt 8.6.3). Det förutsätter givetvis att det inte sker i strid med förbudet i artikel 10 i dataskyddsförordningen. Den som behandlar personuppgifter i strid med artikel 10 kan enligt dataskyddsförordningen drabbas av skadestånd eller administrativa viten.

8.8.2 Praxis och förarbeten angående förbudet

Någon praxis finns av förklarliga skäl inte kring dataskyddsförordningen. I stället lämnas här en redogörelse för den praxis som motsvarande förbud i 21 § personuppgiftslagen gav upphov till. Den praxis som finns avseende 21 § personuppgiftslagen bedöms alltjämt vara relevant och vägledande för förbudet i artikel 10 dataskyddsförordningen. Det erinras dock att i skrivande stund kan Datainspektionen inte uttala sig om misstanke om brott utgör en uppgift som omfattas av förbudet i artikel 10.[50]

[50] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/kansliga-personuppgifter/personuppgifter-som-ror-lagovertradelser/

3 kap. 8 – 9 §§ dataskyddslagen

Av 3 kap. 8 § dataskyddslagen framgår att bara myndigheter får behandla uppgifter om lagöverträdelser, medan det av 3 kap. 9 § framgår att regeringen eller den myndighet som regeringen bestämmer (dvs. Datainspektionen) får medge att även andra får behandla sådana uppgifter.

Forskning som innefattar behandling av personuppgifter om lagöverträdelser m.m. får bara utföras om behandlingen har godkänts enligt lagen (2003:460) om etikprövning av forskning som avser människor. Av 1 § tredje stycket och 15 § lagen (2001:99) om den officiella statistiken följer att sådana myndigheter som är statistikansvariga – vilka dessa är framgår av förordningen (2001:100) om den officiella statistiken – får behandla sådana personuppgifter om lagöverträdelser som avses i artikel 10 dataskyddsförordningen för framställning av officiell och annan statistik bara om det följer av föreskrifter som regeringen meddelar.[51] En statistikansvarig myndighet får alltså inte utan särskilt författningsstöd för framställning av statistik behandla personuppgifter om lagöverträdelser m.m.

Det räcker inte att behandlingen av personuppgifter om lagöverträdelser utförs av myndighet enligt första stycket, av enskild för forskningsändamål med etikgodkännande enligt andra stycket eller med stöd av tillåtelse enligt tredje eller fjärde stycket. För att en behandling av personuppgifter om lagöverträdelser över huvud taget ska få genomföras måste den nämligen också vara *tillåten* enligt någon av de rättsliga grunderna i art. 6.1 dataskyddsförordningen. Också de grundläggande dataskyddsprinciperna i art. 5.1 måste vara beaktade.

Innefattar behandlingen av personuppgifter om lagöverträdelser sådana känsliga personuppgifter som avses i artikel 9.1 dataskyddsförordningen, vilket kan vara fallet t.ex. vid uppgifter om psykiatrisk tvångsvård eller sexualbrott (jämför SOU 2006:82 s. 213), måste även bestämmelserna i artikel 9.2 följas. Innebär behandlingen att personuppgifter om lagöverträdelser förs över till tredjeland, måste också artiklarna 44 - 46 följas.

Det torde ligga i sakens natur att en behandling av personuppgifter om lagöverträdelser som är nödvändig för att *följa* dataskyddsförordningen, t.ex. behandling för att lämna ett registerutdrag enligt artikel 15 dataskyddsförordningen eller för att föra sådan behandlingshistorik (s.k. loggning) som kan vara nödvändig för att uppfylla kraven på säkerhetsåtgärder enligt artikel 32, får utföras av alla personuppgiftsansvariga oberoende av bestämmelserna i denna paragraf.[52]

Förbudet i artikel 10 kan inte upphävas med den registrerades samtycke. Däremot kan regeringen eller den myndighet som regeringen bestämmer (dvs. Datainspektionen) göra undantag från förbudet. En personuppgiftsansvarig som inte

[51] Prop. 2000/01:27 s. 36, 46 ff. och 68, jämför också prop. 2002/03:135 s. 45 f. och 159.
[52] Sören Öman, Hans-Olov Lindblom, Personuppgiftslagen – en kommentar, Zeteo, kommentaren till 21 § PUL.

är en myndighet och som inte heller omfattas av ett undantaget i 3 kap. 8 § dataskyddslagen får således inte behandla personuppgifter om lagöverträdelser ens med den registrerades samtycke.

Däremot har konstitutionsutskottet ansett att det inte finns något hinder mot att den registrerade behandlar uppgifter om sina egna lagöverträdelser m.m. (KU 2000/01:19 s. 16). Länsrätten i Stockholms län har å andra sidan ansett att föräldrar inte kan samtycka till en ideell förening att publicera på nätet uppgifter om tvångsomhändertagna barn.[53]

Förbudet i artikel 10 omfattar personuppgifter som rör brott, fällande domar i ett brottmål, straffprocessuella tvångsmedel, till exempel häktning, reseförbud eller beslag. I det tidigare dataskyddsdirektivet omfattade ett motsvarande förbud behandling av ”uppgifter om lagöverträdelser, brottmålsdomar eller säkerhetsåtgärder” och ”uppgifter som rör administrativa sanktioner”.

Artikel 10 verkar ha ett snävare tillämpningsområde eftersom förbudet omfattar ”fällande domar” och inte brottmålsdomar generellt. Begreppet ”överträdelser” torde motsvara begreppet ”lagöverträdelser” i den tidigare 21 § i personuppgiftslagen, som innehöll ett motsvarande förbud. Det är, som sagt, oklart om misstanke om brott utgör en personuppgift om lagöverträdelse.

De allmänna försäkringskassor som fanns tidigare ansågs som myndigheter.[54] Datainspektionen har ansett att sådana kommunala företag som avses i 2 kap. 3 § offentlighets- och sekretesslagen (dvs. bolag där kommuner har ett rättsligt övervägande inflytande och att bolaget av det skälet ska iaktta bl.a. offentlighetsprincipen) inte är myndigheter vid tillämpningen av denna paragraf.[55] Tillsynen rörde ett kommunalt bostadsföretag och dess e-postkorrespondens mellan personal på bostadsföretaget. E-breven innehöll bl.a. följande: Personalens uppfattningar om dels hyresgäster och tidigare hyresgäster, dels personer som inte har varit hyresgäst hos MKB. Bland annat fanns uppgifter om personers psykiska status. Det framgick exempelvis: ”missbrukare”, ”bosnisk z”, ”svart bryter på franska”. Hela och delar av kriminalregisterutdrag och domar förekom i breven. E-posten hade skrivits ut och satts in i pärmar märkta med ”varningar”. Datainspektionen ansåg att det kommunala bostadsbolaget inte var en myndighet, och därmed träffades av det tidigare förbudet i 21 § personuppgiftslagen.

När det gäller lagöverträdelser har det alltså tidigare enligt svensk uppfattning preciserats att det ska vara fråga om överträdelser som innefattar brott. Varje överträdelse av förhållningsregler i lag omfattas således inte, utan straff måste vara föreskrivet för överträdelsen.[56] Uppgifter om överträdelser som är osanktionerade eller som bara för med sig administrativa sanktioner, t.ex. oriktigt uppgiftslämnande

---

[53] Dom 2004-02-05 i mål nr 1515–02, se om överprövning av den domen Kammarrätten i Stockholms dom 2005-03-30 i mål nr 1872–04

[54] Prop. 2002/03:135 s. 74 och Ds 2002:60 s. 49 och 138.

[55] Beslut 2005-02-15, dnr 82–2005, om behandling av uppgifter om hyresgästers lagöverträdelser m.m. hos Malmös kommunala bostadsföretag, och branschöverenskommelsen om uthyrning av bostäder avsnitt 4.4.1, samt beslut 2013-06-17, dnr 344–346–2013.

[56] Sören Öman, Hans-Olov Lindblom, Personuppgiftslagen – en kommentar, Zeteo, kommentaren till 21 § PUL.

på skatteområdet, otillåtet byggande eller felaktigheter vid miljöfarlig verksamhet, omfattades inte av förbudet i 21 § personuppgiftslagen.[57]

Språkligt sett omfattades bara brottsliga överträdelser av förhållningsregler i lagar och inte brottsliga överträdelser av förhållningsregler i av regeringen beslutade förordningar. Det framgick inte av lagtexten eller förarbetena i vilken utsträckning lagöverträdelser som innefattar brott enligt utländsk lagstiftning omfattas.

En uppgift om att någon har eller kan ha begått något visst brott utgjorde en uppgift om lagöverträdelse, *även om det inte fanns någon dom eller motsvarande beträffande brotte*t. Det är i nuläget dock oklart om förbudet i artikel 10 i dataskyddsförordningen omfattar misstanke om brott.

Datalagskommittén har ansett att uppgifter om *faktiska iakttagelser* om en persons handlande inte rimligen kan anses som uppgifter om lagöverträdelser (SOU 1997:39 s. 383). Som exempel nämnde kommittén en uppgift om att någon använt narkotika, en uppgift om att någon kört bil mellan två orter med viss (för hög) genomsnittlig hastighet, en uppgift om att någon som arbetar med att tömma parkeringsautomater har privat växlat in stora mängder mynt i bank och uppgifter som elektronisk övervakningsutrustning registrerat. Det skulle tala för att uppgifter om sådana händelser inte kvalificerats till att avse något visst brott.

Beträffande exemplet att en uppgift om att någon kört bil mellan två orter med för hög hastighet är enbart en faktisk iakttagelse som, enligt Datalagskommittén, inte utgör en personuppgiftsbehandling i strid med det tidigare förbudet i 21 § personuppgiftslagen, kom Datainspektionen till en annan slutsats i en begäran från Folksam om undantag från förbudet för försöksverksamhet med en apparat i fordonet som avläste hastigheten på försäkringstagarens fordon, och som gav lägre premier om försäkringstagaren höll sig inom rådande hastighetsgränser (Datainspektionens beslut 2012-10-09, dnr 1270-2012).

Inspektionen anförde att av de uppgifter som Folksam avser att behandla kommer det gå att utläsa att den försäkrade bilen har haft en genomsnittshastighet och hur denna hastighet förhåller sig till gällande hastighetsbegränsning på den körda sträckan. Överträdelse av hastighetsbegränsning kommer särskilt markeras som sådan. Datainspektionen var av uppfattningen att uppgiften därmed har kvalificerats till att avse ett visst brott och att den därför inte kan anses utgöra en uppgift om faktiska iakttagelser. Samma bedömning gjorde Datainspektionen i ett beslut om undantag från 21 § rörande Axfood som ville registrera sina lastbilar med GPS-baserad positioneringsteknik som bl.a. registrerar hastigheten på fordonet (beslut 2013-11-18, dnr 768–2013).

Datainspektionen har ansett att följande utgör personuppgifter om lagöverträdelser enligt 21 § personuppgiftslagen:

- Digitala bilder på skadegörelse i form av klotter, om det av bilderna går att utläsa vem som orsakat skadegörelsen, t.ex. genom att klottraren har använt en beteckning på sig själv, en s.k. tag, eller ett gäng klottrare, en s.k. crew (beslut 2005-08-30, dnr 1020–2005, och beslut 2011-04-13, dnr 352–2011)

[57] Ib.

- Digitala bilder på enskilda personer som gripits av ett räddnings- och säkerhetsföretag som misstänkta för skadegörelsebrott (beslut 2006-04-25, dnr 366–2006).
- Uppgifter om att en pantbanks kund tidigare pantsatt stöldgods och att en kund tidigare uppträtt hotfullt på pantbanken (beslut 2005-04-27, dnr 1917–2004).
- Uppgifter om att en hyresgäst på telefon uttalat hotelser mot en anställd på bostadsföretaget när företaget genom att polisanmäla händelsen gjort gällande att det föreligger en misstanke om brott (beslut 2005-06-08, dnr 81–2005).
- Uppgift om s.k. IP-nummer tillsammans med påstående om att innehavaren av numret brutit mot upphovsrättslagen (beslut 2005-06-08, dnr 593–2005, se om överklagande av beslutet dom 2007-06-08 i Kammarrätten i Stockholm i mål nr 285–07, och beslut 2005-10-13, dnr 1019–2005 och 1318–2005, samt beslut 2006-12-15, dnr 1631 och 1632–2006)
- Uppgifter i ett privat företags tjänst på internet för elektronisk polisanmälan med uppgifter om bl.a. misstänkt förövare (beslut 2006-07-10, dnr 706–2006, Länsrätten i Stockholms läns dom 2007-10-24 i mål nr 16617–06).
- Uppgifter om personer som förekommer på USA:s lista över personer med blockerade eller frysta tillgångar (beslut 2006-02-24, dnr 1344–2005).
- Uppgifter och fotografier på personer som skräpar ned vid återvinningsstationer (beslut 2006-10-12, dnr 750–2006). Länsrätten i Stockholm har efter överklagande gjort samma bedömning (dom 2007-10-19 i mål nr 23910–06).
- Uppgifter om e-postadresser och alias på personer som påstås ha begått brott mot barn (beslut 2007-05-02, dnr 1625–2006 och 58–2007).
- Uppgifter om beteendet hos pokerspelare på internet som innefattade en systematisk registrering av spelbeteendet i syfte att upptäcka förekomst av bedrägerier m.m. (beslut 2007-09-21, dnr 424–2007).
- Uppgifter om personer som förekommer på FN:s s.k. terrorlista (samrådsyttrande 2007-11-20, dnr 1239–2007).
- Uppgifter i köp- och säljannonser på internet när behandlingen av personuppgifter skett för att upptäcka försäkringsbedrägerier eller andra brott (beslut 2008-01-28, dnr 886–2007).
- Uppgifter om IP-adresser som använts vid försök till intrång i internetbanker (beslut 2008-03-18, dnr 1402–2007).
- Uppgifter om fordon som tankats på bensinstation utan att tankningen betalats (beslut 2011-05-11, dnr 1563 och 1564–2010, fastställt av Högsta förvaltningsdomstolen, HFD 2016 ref. 8).
- Uppgift om att personer fått tillträdesförbud av åklagare eller avstängts av idrottsorganisation från idrottsevenemang (beslut 2011-05-30, dnr 1841–2010), se också SOU 2012:23.

Förbudet mot behandling av personuppgifter om lagöverträdelser som innefattar brott har inte ansetts hindra att uppgifter om betalningsförsummelser, kreditmissbruk och näringsförbud behandlas i kreditupplysningsverksamhet.[58]

Uppgifter om att någon dömts till straffrättslig påföljd, såsom fängelse eller skyddstillsyn, utgjorde tidigare personuppgifter om lagöverträdelser – eller uppgifter om domar i brottmål – även om det inte av uppgifterna framgår vilken lagöverträdelse som föranlett straffet.

Uppgifter om domar i brottmål omfattades av förbudet i 21 § personuppgiftslagen, även om uppgifterna inte innehöll någon upplysning om en viss lagöverträdelse som innefattar brott. Också en isolerad uppgift om att någon dömts för brott ansågs omfattas av förbudet antingen såsom en uppgift om dom i brottmål eller en uppgift om lagöverträdelse som innefattar brott.

Även uppgifter om civilrättsliga delar av en brottmålsdom omfattades, t.ex. uppgifter om skadeståndsskyldighet som ålagts genom sådan dom. Också en dom i brottmål varigenom någon frikänts omfattades av förbudet i 21 § personuppgiftslagen. Som nämnts har förbudet i artikel 10 dataskyddsförordningen fått en annan utformning; det framgår att förbudet endast omfattar ”fällande” domar i brottmål.

5 § dataskyddsförordningen

Enligt 5 § förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning får personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning behandlas av andra än myndigheter om behandlingen är nödvändig för att
1. rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, eller
2. en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras.
Enligt 6 § får Datainspektionen meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning. Datainspektionen får även i enskilda fall besluta att andra än myndigheter får behandla sådana personuppgifter

Datainspektionen har meddelat sådana föreskrifter som avses i 6 § förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning genom DIFS 2018:2. Härigenom har Datainspektionen föreskrivit att personuppgifter som avses i artikel 10 dataskyddsförordningen får behandlas om

a) det är nödvändig för att fullgöra en föreskrift på socialtjänstområdet,
b) det avser uppgift i anteckningar som förs i fristående skolors elevvårdande verksamhet eller i motsvarande verksamhet hos enskilda anordnare av högskoleutbildning,
c) det är nödvändig för att kontrollera att en jävssituation inte föreligger i advokatverksamhet eller annan juridisk verksamhet, eller

[58] Prop. 2000/01:50 s. 24.

d) det avser personer i nyckelpositioner eller ledande ställning inom det egna bolaget eller koncernen och det är sakligt motiverat att behandla uppgifterna i särskilt inrättade rapporteringskanaler för att utreda om personen ifråga varit delaktig i allvarliga oegentligheter som rör bokföring, intern bokföringskontroll, revision, bekämpande av mutor, brottslighet inom bank- och finansväsen, eller andra allvarliga oegentligheter som rör organisationens vitala intressen eller enskildas liv och hälsa..

Undantaget i 5 § förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning, som tidigare fanns i Datainspektionens föreskrifter om undantag från förbudet i 21 § personuppgiftslagen, har berörts av Datainspektionen i ett antal beslut. Enligt Datainspektionen uppfattning måste höga krav ställas på de situationer i vilka undantagen från de principiella förbud som finns mot att behandla känsliga personuppgifter och brottsuppgifter tillämpas. Uppgifterna måste då vara hänförliga till ett konkret rättsligt anspråk och all behandling som sker måste vara nödvändig i förhållande till detta anspråk. Behov av att samla uppgifter inom ett bostadsföretag rörande hyresgäster, exempelvis som grund för avhysning, bör kunna tillgodoses genom att beskriva händelser och iakttagelser istället för uttryckliga uppgifter om sjukdom och psykisk status (beslut 2005-02-15, dnr 82–2005).

Ett par offentliga försvarare i ett omfattande brottmål, där åklagaren bl.a. åberopat 114 vittnesförhör, ansökte om undantag för att få tillgång till förundersökningen i målet i digital form (beslut 2003-05-12, dnr 757–2003). Datainspektionen anförde: ”Syftet med undantaget [...] är att göra det möjligt för bl.a. advokater att behandla personuppgifter om klienter som exempelvis är misstänkta för brott. Nödvändiga behandlingar av personuppgifter som exempelvis rör försvaret av klienten vid misstanke om brott omfattas av undantaget. Är det nödvändigt för försvaret av klienten är det även tillåtet att behandla uppgifter om eventuella medåtalade. Er behandling av brottsuppgifter som har betydelse för att utföra ert uppdrag omfattas av undantaget [...] och är därmed tillåten. Huruvida personuppgifterna som behandlas samlas in från diskett, cd-romskiva eller från papper saknar betydelse vid tillämpningen av denna undantagsbestämmelse. En förutsättning för att behandlingen ska vara laglig är emellertid att endast nödvändiga och relevanta uppgifter samlas in t.ex. från en cd-romskiva som innehåller förundersökningen. Med hänsyn till ovanstående anser Datainspektionen att det inte behövs något särskilt beslut om undantag från 21 § PUL. Ansökan skall därför avvisas.”

I ett annat fall hade ett bostadsföretag registrerat uppgifter om att en hyresgäst hotat företagets personal (beslut 2005-06-08, dnr 81–2005). Datainspektionen ansåg att uppgifterna med stöd av bestämmelsen – och efter en intresseavvägning enligt 10 § f personuppgiftslagen (art. 6.1 f i dataskyddsförordningen) – kunde behandlas i samband med uppsägning av ett hyreskontrakt eller vid författandet av en polisanmälan. Datainspektionen tillade: ”Om uppgifterna avser en händelse som den personuppgiftsansvarige bedömer inte behöver föranleda någon åtgärd nu kan en rapport om saken upprättas med stöd av samma bestämmelser. En förutsättning för

det är att händelsen är nödvändig för att i ett senare skede framställa ett rättsligt anspråk, exempelvis som grund för uppsägning.” Antipiratbyrån hade behandlat bl.a. uppgifter om s.k. IP-nummer för personer som misstänktes olovligen sprida upphovsrättsligt skyddat material på internet och under ett år gjort 136 polisanmälningar och varje dag sänt 1 500–2 000 varningsbrev. Det har numera införts bestämmelser i varumärkeslagen, upphovsrättslagen, patentlagen, mönsterskyddslagen, firmalagen, kretsmönsterlagen och växtförädlarrättslagen om att personuppgifter om lagöverträdelser som innefattar brott mot dessa lagar får behandlas om detta är nödvändigt för att ett rättsligt anspråk ska kunna fastställas, göras gällande eller försvaras.[59] Därvid har det i förarbetena framhållits att det rättsliga anspråket måste vara konkret, dvs. avse ett eller flera specifika intrång och att bestämmelserna alltså inte ger rättighetshavarna någon rätt att upprätta ett systematiskt register över sådana internetanvändare som misstänks syssla med t.ex. olaglig fildelning.

I ett fall har Datainspektionen utgått från att innebörden av ”rättsliga anspråk” är densamma som enligt 16 § första stycket c i den tidigare personuppgiftslagen (beslut 2002-10-23, dnr 1579–2002). Att det krävts enligt lagstiftning i USA för att få bedriva viss verksamhet att ett moderbolag i USA redovisar brottslighet hos anställda hos dotterbolag i Sverige har inte ansetts innebära att uppgifterna om brottsligheten är nödvändiga för att rättsliga anspråk ska kunna fastställa, göras gällande eller försvaras i ett enskilt fall (Datainspektionens beslut 2007-12-18, dnr 764–2007).

Enligt 6 § kreditupplysningslagen (1973:1173) kan Datainspektionen, om det finns synnerliga skäl, medge att personuppgifter om lagöverträdelser m.m. behandlas i kreditupplysningsverksamhet.[60]

Privata arbetsgivare som tar hand om barn har skyldighet att hämta in registerutdrag om brottslighet före anställning m.m. enligt 2 kap. 31–33 §§ skollagen (2010:800) (tidigare lagen [2000:873] om registerkontroll av personal inom förskoleverksamhet, skola och skolbarnsomsorg) (prop. 1999/2000:123, UbU 2000/01:4 och SOU 1998:69 samt prop. 2007/08:28 och Ds 2004:42), lagen (2007:171) om registerkontroll av personal vid sådana hem för vård eller boende som tar emot barn (prop. 2006/07:37, SoU 2006/07:9 och SOU 2005:65) och lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder (prop. 2009/10:176, SoU 2009/10:21 och SOU 2008:77). Se också Skolverkets rapport 2003-05-20 om uppföljning av lagen avseende personal inom förskoleverksamhet, skola och skolbarnsomsorg, dnr 01–2002:1807. Jämför Ds 2012:45 för förslag om, inte en skyldighet utan, en uttrycklig lagstadgad rätt för arbetsgivare att i vissa fall begära registerutdrag, något som sedan ändrades till en skyldighet för arbetssökanden att på begäran visa upp ett utdrag (prop. 2012/13:194), se lagen (2013:852) om registerkontroll av personer som ska arbeta med barn. Jämför SOU 2014:3 om registerkontroll av personer som ska ta emot barn i sitt hem för omvårdnad och fostran.

---

[59] Prop. 2008/09:67 s. 172 f. och 269.
[60] Prop. 2000/01:50 s. 23 f.

Beträffande anställda försäkringsförmedlare gäller en motsvarande skyldighet enligt 2 kap. 6 § lagen (2005:405) om försäkringsförmedling (prop. 2004/05:133 s. 65 ff.), varvid dock i 3 kap. 3 § förordningen (2005:411) om försäkringsförmedling uttryckligen föreskrivits att försäkringsföretaget inte får dokumentera den utförda kontrollen på annat sätt än genom en anteckning om att registerutdraget har visats upp.

Det har föreslagits ett förbud för arbetsgivare att utan författningsstöd begära att arbetstagare, arbetssökande eller inhyrd personal visar upp utdrag ur belastnings- eller misstankeregistret (SOU 2009:44), men det har inte genomförts. Frågan om registerutdrag i arbetslivet har i stället utretts på nytt och samma förslag lämnats igen (SOU 2014:48 och dir. 2013:56). Patientsäkerhetsutredningen föreslog att det skulle införas en lag om registerkontroll vid anställning av personal inom hälso- och sjukvården (SOU 2008:117), men regeringen ansåg att det inte borde införas en sådan lag (prop. 2009/10:210 s. 165 ff.).

Jämför också tidigare lagen (1999:163) om penningtvättsregister (prop. 1998/99:19, JuU 1998/99:8 och SOU 1997:36 samt prop. 2003/04:156 s. 59) och lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m. (prop. 2001/02:149 och JuU 2001/02:25) samt numera 4 kap. lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism (prop. 2008/09:70 och SOU 2007:23).

Jämför om bankers och andra betaltjänstleverantörers granskning av betalningstransaktioner för att upptäcka bedrägerier lagen (2010:751) om betaltjänster (prop. 2009/10:220 s. 261 ff.).

Genom 6 § förordningen om kompletterande bestämmelser till EU:s dataskyddsförordning har regeringen bemyndigat Datainspektionen att meddela undantag från förbudet i artikel 10 i enstaka fall. Enskilda personuppgiftsansvariga kan således ansöka hos Datainspektionen om undantag för vissa bestämda behandlingar av sådana personuppgifter som avses i artikel 10 som de avser att genomföra.

Enligt Datainspektionens tidigare mening ska möjligheten att meddela undantag tillämpas restriktivt (t.ex. beslut 2005-08-30, dnr 1020–2005, beslut 2005-10-13, dnr 1019–2005 och 1318–2005, beslut 2006-02-24, dnr 1344–2005, beslut 2008-03-26, dnr 1202–2007, och beslut 2013-11-18, dnr 768–2013). Högsta förvaltningsdomstolen har delat den bedömningen (HFD 2016 ref. 8).

Datainspektionen har tidigare meddelat beslut om undantag för ett företag för kollektivtrafik – Storstockholms Lokaltrafik, SL – som ville registrera uppgifter om klotter, bl.a. digitala bilder, och klottrare i en databas med omkring 60 000 registreringar per år för att fastställa, göra gällande och försvara rättsliga anspråk med anledning av klottret, t.ex. polisanmälningar och skadeståndsanspråk (beslut 2005-08-30, dnr 1020-2005, se också beslut 2005-12-21, dnr 1642-2005, och beslut 2006-09-15, dnr 884-2006, samt beslut 2011-04-13, dnr 352-2011, om SJ:s motsvarande databas). Datainspektionen anförde därvid följande:

”Det är endast fråga om att registrera de digitala bilder som tagits av skadegörelsen och den eventuella text som kan framgå av skadegörelsen. De enda personuppgifter som kan komma att behandlas i detta sammanhang och i vissa fall betraktas som personuppgifter om lagöverträdelser är den text som kan framgå av bilden och som klottraren själv skrivit. Det av SL beskrivna tillvägagångssättet ger inte utrymme för att registrera ytterligare information såsom t.ex. brottsmisstankar eller värdeomdömen om namngivna personer som skulle kunna vara integritetskränkande. Uppgifterna kommer endast att bevaras till dess att ett ärende blivit uppklarat, som längst i två år.”

Registrering av klotter i form av bilder torde numera omfattas av undantaget i 5 § 1 förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning (rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras). Den tidigare begränsningen som fanns i Datainspektionens föreskrifter om att enbart ”enstaka” personuppgifter får registreras är för dessa syften är borttagen.

Datainspektionen har tidigare meddelat beslut om tidsbegränsade undantag för två organisationer – Antipiratbyrån och IFPI – som bedriver s.k. antipiratverksamhet, dvs. behandlar bl.a. uppgifter om s.k. IP-nummer för personer som misstänks olovligen sprida upphovsrättsligt skyddat material på internet i syfte att få spridningen att upphöra och att civil- och straffrättsligt beivra intrången (beslut 2005-10-13, dnr 1019-2005 och 1318-2005, och beslut 2006-12-15, dnr 1631 och 1632-2006, samt beslut 2008-12-19, dnr 1757-2008 och 1814-2008). I beslutet angående Antipiratbyrån (dnr 1019–2005) anförde Datainspektionen:

”När det gäller Antipiratbyråns begäran om undantag från förbudet att behandla uppgifter om lagöverträdelser, finns ett antal faktorer, som är relevanta för prövningen. Följande omständigheter talar särskilt mot att medge undantag:

- Många Internetanvändare kan uppleva Antipiratbyråns hantering som ett otillbörligt integritetsintrång.
- Sammantaget är det fråga om en omfattande behandling av personuppgifter.
- Det finns en risk att vissa mottagare av de s.k. varningsbreven är fullständigt oskyldiga.

Följande faktorer talar särskilt för att medge det begärda undantaget:

- Antipiratbyrån har i uppdrag av sina medlemmar att tillvarata deras intressen vid brott mot upphovsrätten.
- De aktuella personuppgifterna översänds enbart till berörd Internetleverantör eller i vissa fall till polis och domstol.
- Antipiratbyrån har beskrivit att man endast eftersöker information om upphovsrättskyddade verk som en person otillåtet tillgängliggjort i sådana förteckningar, som personen redan genom att ingå i ett s.k. fildelningsnätverk, gjort tillgängliga för omvärlden.
- Antipiratbyrån identifierar inte vem som har använt ett visst IP-nummer.

Datainspektionen bedömer att Antipiratbyrån har ett befogat intresse att utföra de begärda behandlingarna av personuppgifter och de beskrivna behandlingarna får anses vara proportionerliga med hänsyn till det syfte behandlingen avser. Det är inte

fråga om att upprätta ett systematiskt register över sådana Internetanvändare som misstänks syssla med otillåten fildelning och uppgifterna kommer inte att sparas längre än vad som är nödvändigt. Vidare kan konstateras att uppgifter om anknytningen mellan en IP-adress och en Internetanvändare inte tas fram av Antipiratbyrån. Slutligen bedömer Datainspektionen att det eventuella integritetsintrånget begränsas av att det enbart avser sökning i förteckningar, som i princip är tillgängliga för alla Internetanvändare, som anslutit sig till ett ”fildelningsnätverk”.

- Datainspektionen har meddelat beslut om tidsbegränsade undantag för banker att kontrollera kunders utlandsbetalningar mot USA:s lista över personer med blockerade eller frysta tillgångar, den s.k. OFAC-listan (beslut 2006-02-24, dnr 1344–2005, och beslut 2007-09-17, dnr 864–2007; se härom SOU 2007:23 s. 153 f. och prop. 2008/09:70 s. 136 f.). Sedermera har Datainspektionen meddelat bankerna ett undantag tills vidare (beslut 2010-09-16, dnr 589–2010). Beslutet har meddelats under det uttryckliga villkoret, att det under vissa betingelser kan komma att återkallas.
- Däremot har Datainspektion avslagit en begäran från flera svenska dotterbolag i en internationell koncern som bl.a. sysslar med finansiering om att få kontrollera om potentiella kunder, anställda med flera finns på olika (svarta) listor som myndigheter i USA fastställt. Avslagsbeslutet har upprätthållits efter överklagande (Kammarrättens i Stockholm dom 2016-04-13 i mål nr 3946–3958–15).
- Datainspektionen har meddelat beslut om tidsbegränsade undantag för banker att systematiskt behandla och utbyta uppgifter om IP-adresser som använts vid försök till intrång i internetbanker (beslut 2008-03-18, dnr 1402–2007, och beslut 2009-02-24, dnr 138–2009).
- Datainspektionen har meddelat beslut om undantag för Svenska Spel att genomföra en systematisk registrering av pokerspelares spelbeteende vid pokerspel på internet i syfte att upptäcka förekomst av bedrägerier m.m. (beslut 2007-09-21, dnr 424–2007).
- Datainspektionen har meddelat beslut om undantag för idrottsorganisation att ha en databas över personer som fått tillträdesförbud av åklagare eller avstängts av idrottsorganisation från idrottsevenemang (beslut 2011-05-30, dnr 1841–2010).
- Datainspektionen har meddelat beslut om undantag för ett försäkringsföretag att registrera hastighetsöverträdelser för att kunna bestämma bilförsäkringspremie efter hur fordonet framförts (beslut 2012-10-09, dnr 1270–2012). Se mer härom ovan.
- Datainspektionen har meddelat beslut om undantag för ett distributionsföretag att med hjälp av GPS registrera anställda förares hastighetsöverträdelser i syfte att genom en upplysningsskärm i fordonet och efterföljande samtal med föraren öka trafiksäkerheten (beslut 2013-11-18, dnr 768–2013). Se mer härom ovan.

- Datainspektionen har meddelat beslut om undantag för Larmtjänst AB att i uppskattningsvis 10–20 fall per år behandla personuppgifter i köp- och säljannonser på internet för att på uppdrag av försäkringsbolag upptäcka försäkringsbedrägerier eller andra brott (beslut 2008-01-28, dnr 886–2007).
- Datainspektionen har meddelat beslut om undantag för ett svenskt företag i en internationell koncern för att införa ett koncerngemensamt system för s.k. whistleblowing (för visselblåsare) och där behandla personuppgifter om allvarliga oegentligheter avseende nyckelpersoner och personer i ledande ställning för att säkerställa att koncernen agerar lagligt och i överensstämmelse med etiska riktlinjer (beslut 2008-03-26, dnr 1202-2007, jämför Förvaltningsrätten i Stockholms domar 2010-03-12 i mål nr 12584-10, 23861-10 och 23863-10). Per den 1 november 2010 har det införts ett generellt undantag för system för whistleblowing.
- Datainspektionen har avslagit ansökningar från revisionsbyråer om att få registrera bl.a. revisorers brottmålsdomar för att föra över uppgifterna till myndigheter i USA (beslut 2004-04-07, dnr 377 och 469–2004).
- Datainspektionen har vidare avslagit ett värderingsföretags ansökan om att få registrera uppgifter om företagets anställda dömts för brott för att överföra uppgifterna till moderbolaget i USA så att det ska kunna få tillstånd från myndigheter i USA att tillhandahålla värderingstjänster (beslut 2007-12-18, dnr 764–2007).
- Datainspektionen har avslagit en ansökan från en pantbank om att få registrera att kunder pantsatt stöldgods tidigare och att kunder tidigare uppträtt hotfullt på pantbanken (beslut 2005-04-27, dnr 1917–2004).
- Datainspektionen har avslagit ansökningar som innebar att många olika bensinstationer skulle rapportera in uppgifter om fordon, vars registreringsnummer automatiskt registrerats med hjälp av s.k. LPR-kameror och som tankats utan att tankningen betalats, till ett säkerhetsföretag som skulle registrera dessa uppgifter och uppgifter om fordonsägarna i en databas och lämna ut dem om någon försökte tanka fordonet på en ansluten bensinstation (beslut 2011-05-11, dnr 1563 och 1564–2010). Högsta förvaltningsdomstolen har fastställt det avslagsbeslutet (HFD 2016 ref. 8).

Under åren 2008–2010 ökade antalet ansökningar om undantag kraftigt, från ungefär tio eller färre ansökningar per år till 76 ansökningar år 2010.[61] De allra flesta ansökningarna 2010, 66 stycken, avsåg system för whistleblowing (för visselblåsare). Numera har det som sagt införts ett generellt undantag för system för whistleblowing som bygger på de beslut i enskilda fall som tidigare meddelats.

8.8.3 Överväganden

[61] Sören Öman, Hans-Olov Lindblom, Personuppgiftslagen – en kommentar, Zeteo, kommentaren till 21 § PUL

Som framhållits tidigare i denna framställning är Embrace ett verktyg eller stöd för att bedriva lokalt brottsförebyggande arbete i samverkan mellan olika aktörer. Syftet med tjänsten är inte att registrera individer utan händelser förknippade med brottsliga eller andra otrygghetsskapande händelser. Det behöver inte röra sig om polisanmälda brott. Embrace registrerar emellertid platsen för händelsen, vilket i vissa fall kan vara en gatu- eller fastighetsadress, vilken uppgift indirekt kan hänföras till enskilda fysiska personer, t.ex. personer som drabbat av en skadegörelse, hot eller ett fysiskt angrepp (se avsnitt 8.1). Slutsatsen som dragits i denna laglighetsprövning är att Embrace i vissa fall hanterar ”personuppgifter”, särskilt när gatu- och adressuppgifter registreras. Däremot inte när händelser på allmänna platser, ett torg, registreras.

Frågan som nu är för handen är om uppgifter av det slag som registreras av Embrace omfattas av förbudet i artikel 10 dataskyddsförordningen, som hade en motsvarighet i 21 § personuppgiftslagen. Enligt artikeln får enbart myndigheter behandla personuppgifter som rör brott, fällande domar i brottmål samt straffprocessuella tvångsmedel, t.ex. häktning, reseförbud och beslag (lagöverträdelser).

I det föregående har polisen liksom kommuner bedömts vara potentiella användare av Embrace. De kommunala nämnderna och Polismyndigheten är myndigheter och får därmed hantera aktuella uppgifter i Embrace. De träffas så att säga inte av förbudet i artikel 10 i dataskyddsförordningen, men ska givetvis i övrigt beakta andra krav i dataskyddsförordningen, bl.a. de grundläggande principerna i art. 5 såsom att bara registrera adekvata och relevanta uppgifter samt i så stor utsträckning arbeta med pseudonymiserade uppgifter.

En annan målgrupp för Embrace är bostads- och fastighetsbolag som arbetar aktivt med trygghetsfrågor för sina hyresgäster i boendemiljön. Det är här fråga om privata aktörer, inte myndigheter. De träffas därmed av förbudet i art. 10.

Av det skälet har ett flertal frågor ställts som ska besvaras.

- Får rapportering, inklusive fotografering av skadegörelse på skolor, bostäder och kommersiella fastigheter registreras i Embrace, t.ex. klotter?
- Omfattar förbudet i artikel 10 enbart uppgifter om förövaren, men inte uppgifter om brottsoffren?
- Får en privat aktör, exempelvis ett kommunalt bostadsbolag, behandla personuppgifter rörande förövaren respektive brottsoffret i Embrace om det finns en samverkan med en myndighet, t.ex. polisen.

Till att börja med kan konstateras att kommunala fastighetsbolag, där kommunen har ett rättsligt övervägande inflytande, såsom t.ex. aktiemajoritet, inte utgör myndigheter i förvaltningslagens bemärkelse och av det skälet inte kan undgå att träffas av förbudet i artikel 10 i dataskyddsförordningen (se avsnitt 8.6).

Inte alla händelser som registreras i Embrace omfattas nödvändigtvis av förbudet i artikel 10 i dataskyddsförordningen. Enligt tidigare praxis måste straff vara föreskrivet för överträdelsen, och regleringen ska finnas i lag. Det är oklart i vilken utsträckning tidigare praxis är alltjämt giltig med det snävare tillämpningsområde

som förbudet i artikel 10 har i jämförelse med förbudet i 21 § personuppgiftslagen. I nuläget är det t.ex. oklart om misstanke om brott träffas av förbudet.[62]

Majoriteten av händelserna som registreras i Embrace kan man dock räkna med utgör s.k. brottsbalksbrott, t.ex. skadegörelse i olika former, stöld, hot och misshandel. De torde omfattas därmed av förbudet per se.

Vidare registreras inga uppgifter om misstänkta personer. De uppgifter som registreras kan däremot härledas indirekt till berörda brottsoffer.

De händelser som registreras i Embrace utgör faktiska iakttagelser av lagöverträdelser. Datalagskommittén har uttalat att sådana iakttagelser normalt inte ska omfattas av förbudet i 21 § PUL.[63] Återigen är det oklart om sådana uttalanden alltjämt har giltighet för dataskyddsförordningens bestämmelser. I brist på annan vägledning bör denna uppfattning fortfarande anses vara relevant.

Som redovisats har Datainspektionen ansett i två fall att en uppgift om att någon körd bil mellan två orter med för hög hastighet, vilken uppgift registrerats av en teknisk lösning i fordonet, inte utgör en faktisk iakttagelse. I besluten[64] noterade Datainspektionen att överträdelsen av hastighetsbegränsningen *markeras särskilt i lösningen*. Datainspektionen var av uppfattningen att uppgiften därmed har kvalificerats till att avse ett visst brott och att den därför inte kan anses utgöra en uppgift om faktiska iakttagelser.

Några sådana särskilda markeringar om brott förekommer inte Embrace. Embrace validerar inte om en händelse uppfyller rekvisiten för brott utan registrerar en bild av var och när saker sker. Å andra sidan registrerar Embrace konsekvenserna av ett brott, såsom en krossad fönsterruta i en fastighet eller stöld av viss egendom, t.ex. en dator i en skola. Det skulle tala för att uppgifterna i och för sig kvalificerar sig som brott.

En fråga är dock vems uppgifter förbudet i artikel 10 i dataskyddsförordningen tar fasta på. Den som misstänks eller har dömts för ett brott och/eller brottsoffer?

Datalagskommittén anför beträffande förbudet att ”[e]n uppgift om att någon har eller kan ha begått ett visst brott utgör en uppgift om lagöverträdelse, även om det inte finns någon dom eller motsvarande beträffande brottet, om uppgiften har kvalificerats till att avse något visst brott.[65]

På Datainspektionens tidigare hemsida fanns frågor och svar. En sådan fråga avsåg registrering av uppgifter om brott. Inspektionen anförde bl.a. följande: ”Att föra register över personer som misstänks ha begått något brott är således enligt huvudregeln i 21 § personuppgiftslagen förbjudet för andra än myndigheter och det krävs inte att personen är anmäld eller dömd för att förbudet ska gälla.”[66]

Inte i något fall har i litteraturen eller Datainspektionens praxis framförts uppfattningen att förbudet i 21 § personuppgiftslagen omfattar brottsoffer.

---

[62] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/kansliga-personuppgifter/personuppgifter-som-ror-lagovertradelser/
[63] SOU 1997:39 s. 383.
[64] Datainspektionens beslut 2012-10-09, dnr 1270–2012 och 2013-11-18, dnr 768–2013.
[65] SOU 1997:39 s. 380.
[66] Frågan är borttagen från Datainspektionens hemsida.

(Uppgifterna om brottsoffer kan dock av andra skäl inte få behandlas enligt dataskyddsregler.)

Övervägande skäl talar således för att förbudet i artikel 10 inte omfattar registrering av brottsrelaterade händelser i Embrace som kan i vissa fall indirekt hänföras till fysiskt levande personer som drabbats av händelsen eller är ägare av egendom eller representant för en sådan ägare som berörs av händelsen. Det utesluter inte givetvis, såsom berörs i avsnitt 8.1, att det kan föreligga risker för enskildas friheter och rättigheter vid behandling av dessa uppgifter, vilket förutsätter att uppgifterna hanteras inom ramen för dataskyddsförordningens bestämmelser.

Sammanfattningsvis och vid en sammantagen bedömning bedöms förbudet i artikel 10 i dataskyddsförordningen, inte vara tillämpliga på majoriteten av uppgifter som registreras som text eller bild i Embrace eftersom förbudet tar fasta på uppgifter om den som begått ett brott och inte uppgifter om brottsoffer. Beträffande bilder på klotter, se nedan.

Även 5 § i förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning ska kort kommenteras. I förordningen finns två undantag från förbudet i artikel 10. Inget av undantagen är tillämpligt på Embrace. Beträffande ett av undantagen, rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, så avser det enbart registrering av personuppgifter som är nödvändig enbart i syfte att göra rättsliga anspråk. Som redovisats måste det röra sig ett konkret rättsligt anspråk och all behandling som sker måste vara nödvändig i förhållande till detta anspråk. Som exempel nämner Datainspektionen bostadsföretag som har behov av att samla uppgifter rörande hyresgäster, exempelvis som grund för avhysning (beslut 2005-02-15, dnr 82–2005). Datainspektionen förklarar att det bör kunna tillgodoses genom att beskriva händelser och iakttagelser istället för uttryckliga känsliga personuppgifter, t.ex. om sjukdom och psykisk status.

Embrace är inget brottsutredande verktyg utan brottsförebyggande. Det är inte designat för att göra rättsliga anspråk, och av det skälet är undantaget i förordningen inte tillämplig.

En annan fråga rör bilder på klotter. Det är en specialsituation som måste uppmärksammas i sammanhanget. Av Datainspektionens praxis framgår att digitala bilder på skadegörelse i form av klotter inte får registreras, om det av bilderna går att utläsa vem som orsakat skadegörelsen, t.ex. genom att klottraren har använt en beteckning på sig själv, en s.k. tag, eller ett gäng klottrare, en s.k. crew (beslut 2005-08-30, dnr 1020–2005, och beslut 2011-04-13, dnr 352–2011).

Sådana bilder omfattades tidigare inte av Datainspektionens undantag i DISF 1998:32:2. Därför meddelade Datainspektionen i ett fall rörande Storstockholms lokaltrafik ett undantag för registrering av bilder av klotter och klottrare i en databas med omkring 60 000 registreringar för att fastställa, göra gällande och försvara rättsliga anspråk med anledning av klottret, t.ex. polisanmälningar och skadeståndsanspråk.

Numera finns undantaget för andra än myndigheter att få behandla personuppgifter om lagöverträdelser för att fastställa, göra gällande och försvara

rättsliga anspråk i 5 § 1 förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning. Utgångspunkten är att undantaget är tillämpligt på bilder av klotter.

Som redovisats i avsnitt 2.2 registreras i Embrace som regel bara händelser om vad, var, när och åtgärd. Bilder kan också registreras, men enbart med syfte att följa upp insatser på platser som är särskilt drabbade av brottsrelaterade och andra otrygghetsskapande händelser. Det kan röra sig om bilder på klotter eller annan skadegörelse samt förändringar i miljön som vidtagits för att undvika klotter.

För Embrace står här tre alternativ till buds:

- Förhindra registrering av bilder i Embrace
- Informera fastighets- och bostadsbolag och andra aktörer som vill köpa Embrace om att
    - enbart fotografera klottret men inte taggen, eller
    - ansöka hos Datainspektionen om undantag från förbudet i artikel 10dataskyddsförordningen för att kunna lägga in bilder om klotter.

Det första alternativet framstår inte som ett realistiskt alternativ. Återstår det andra alternativet, dvs. att de fastighets- och bostadsföretag som nyttjar Embrace informeras vid köp samt i applikationen om de särskilda begränsningar som råder för fotografering av klotter och vilka kompensatoriska mekanismer som kan vidtas samt erinra dem om deras personuppgiftsansvar.

Det är dock på sin plats att uppmärksammas, liksom i avsnitt 8.6 avseende fritextrutorna och riskerna med dessa för registrering av känsliga personuppgifter, att dataskyddsförordningen ställer krav på att personuppgiftsansvariga arbetar aktivt med privacy by design och privacy by default, art. 25.1 och 25.2 (se avsnitt 8.6.1). Motsvarande krav finns i 3 kap. 3 - 4 §§ brottsdatalagen. Det innebär att Embrace måste innehålla mekanismer som säkerställer att det inte uppstår en risk för registrering av bilder som visar vem gärningsmannen är.

Redan i dag har emellertid Embrace utbildning samt tekniska och administrativa funktioner på plats i Embrace som ska förhindra att individuppgifter alternativt känsliga personuppgifter registreras i tjänsten. Utbildningen och kontrollen bör även uppmärksamma att bilder på taggar på klotter och modus operandi som utvisar misstänkt gärningsman kan utgöra personuppgifter om lagöverträdelser. Sådana uppgifter får inte förekomma i Embrace om tjänsten används av privata aktörer inom näringslivet.

Embrace bör givetvis friskriva sig i avtal från ansvar för privata aktörers registrering av bilder som kan visa vem gärningsmannen är.

Ett problem som bör uppmärksamma här är att kommuner och polisen får lagligen registrera bilder i egenskap av myndigheter som utvisar taggar och crew. Det måste finnas filter eller begränsningar i Embrace som förhindrar att sådana uppgifter delas med bostads- och fastighetsföretag eller andra privata aktörer vilka man samverkar med lokalt. Det skulle kunna innebära en stående rutin att administratörerna som granskar registrerade uppgifter alltid suddar ut eller pixlar taggar som syns på digitala foton över klotter.

Embrace Safety AB bör informera och utbilda kommuner och polisen om att de inte får dela bilder i Embrace Insight (den lokala gemensamma problembilden) med privata användare som utvisar vem som begått ett brott. En sådan delning kan vara straffbart. Även i detta fall rekommenderas Embrace Safety AB att implementera mekanismer i själva tjänsten som förhindrar sådan informationsöverföring till privata aktörer

8.9 Är RPSFS 2012:18 och förordningen om bevakningsföretag tillämplig på Embrace?

Bedömning: Lagen om bevakningsföretag och vidhängande författningar är inte tillämpliga på verksamhet med stöd av Embrace.

En fråga som ställs är om lagen (1974:191) och förordningen (1989:149) om bevakningsföretag samt Rikspolisstyrelsens föreskrifter och allmänna råd RPSFS 2012:18 är tillämpliga på Embrace, dvs. om den aktör som använder Embrace rent formellt måste ha auktorisation från länsstyrelsen eftersom det rör sig om en verksamhet som syftar till förbättrat skydd?

Av 1 § i lagen om bevakningsföretag framgår att med bevakningsföretag avses i lagen den som yrkesmässigt åtar sig att för annans räkning

1. bevaka fastighet, anläggning, viss verksamhet, offentlig tillställning eller något annat sådant,
2. bevaka enskild person för dennes skydd, eller
3. bevaka sedlar, mynt eller annan egendom i samband med transport.

Det följer redan av kravet på yrkesmässighet att lagen inte är tillämplig på en aktör som använder Embrace. Av lagens 1 § framgår vidare att lagen inte är tillämplig på bevakning som utförs av kommun och landsting.

För övrigt är Embrace inte ett övervakningsverktyg utan ett verktyg för brottsförebyggande arbete på lokal nivå och i samverkan mellan flera aktörer.

9 Övriga skyldigheter och rättigheter

I detta kapitel övervägs andra aspekter på behandlingen av personuppgifter i Embrace, såsom information till registrerade och deras rättigheter enligt dataskyddsförordningen. Informationen i detta kapitel berör i huvudsak Embraces kunder.

9.1 Information till den registrerade

Dataskyddsförordningen lägger stor vikt vid transparens. Det ska aldrig komma som en överraskning för någon att en aktör behandlar ens personuppgifter eller för vilket syfte. Kravet på transparens kommer till uttryck i de grundläggande dataskyddsprinciperna i dataskyddsförordningen, art. 5.1 a (se avsnitt 8.5). En personuppgiftsansvarig ska vidare kunna ”visa” att kravet på transparens är uppfyllt gentemot de registrerade (art. 5.2). Den 28 november 2017 har Artikel 29-arbetsgruppen publicerat en vägledning om informationsskyldigheten enligt dataskyddsförordningen.[67]

Det erinras att om kravet på information i dataskyddsförordningen inte är uppfylld, kan personuppgiftsbehandlingen betraktas som otillåten, oavsett att behandlingen i övrigt uppfyller förordningens krav. Brister i informationsplikten kan således föranleda administrativa vitessanktioner mot den personuppgiftsansvarige.

Bestämmelser om information till de registrerade finns i artiklarna 12.1, 13 och 14. Av art. 12.1 framgår att den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34 vilken avser behandlingen ska lämnas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn.

Artikel 12.1 stipulerar vidare att informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen enligt artikeln tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

Av skäl 61 framgår att information om behandling av personuppgifter som rör den registrerade bör lämnas till honom eller henne vid den tidpunkt då personuppgifterna samlas in från den registrerade eller, om personuppgifterna erhålls direkt från en annan källa, inom en rimlig period, beroende på omständigheterna i fallet. Om personuppgifter legitimt kan lämnas ut till en annan mottagare, bör de registrerade enligt skäl 61 informeras första gången personuppgifterna lämnas ut till

[67] Guidelines on transparency under Regulation 2016/679 (EN/17).

denna mottagare. Om den personuppgiftsansvarige avser att behandla personuppgifter för ett annat ändamål än det för vilket uppgifterna insamlades, bör denne enligt samma skäl före ytterligare behandling informera den registrerade om detta andra syfte och lämna annan nödvändig information. Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, bör allmän information ges.

Vad som ska informeras när uppgifter samlas in från den registrerade själv framgår av art. 13. Av art. 14 framgår vilken information som ska lämnas till den registrerade om uppgifterna har samlats in från en tredje part, t.ex. andra personuppgiftsansvariga eller andra registrerade.

Det är en tämligen omfattande katalog av informationspunkter som faller in under de båda informationsskyldigheterna. Framställningen hänvisar till förordningen i denna del. Bl.a. ska information om ändamålet för personuppgiftsbehandlingen lämnas och vem som står bakom behandlingen.

Dataskyddsförordningen innehåller även undantag från informationsskyldigheten. Om den registrerade redan förfogar över informationen om personuppgiftsbehandlingen och vem som behandlar dennes personuppgifter behöver inte information lämnas (se art. 13 och 14). Undantaget är tillämpligt oavsett om uppgifterna samlats in från den registrerade eller från någon annan än den registrerade. Givetvis måste den personuppgiftsansvarige kunna ”visa” att den registrerade redan har fått information om personuppgiftsbehandlingen, bl.a. på vilket sätt och när, och att inte personuppgiftsbehandlingen förändrats sedan dess för att kunna undgå sin informationsplikt.

När det gäller informationsskyldigheten enligt art. 14, dvs. när den personuppgiftsansvarige får personuppgifter från någon annan än den registrerade, finns ytterligare undantag från informationsskyldigheten. I sådana fall kan informationsskyldigheten underlåtas om

- tillhandahållandet av sådan information visar sig vara omöjligt,
- tillhandahållandet av sådan information skulle medföra en oproportionell ansträngning, särskilt för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1,
- informationsskyldigheten sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av målen med behandlingen; i sådana fall ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, inbegripet göra uppgifterna tillgängliga för allmänheten,
- erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom nationella rätt som den registrerade omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen, eller

- personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller nationell rätt, inbegripet andra lagstadgade sekretessförpliktelser

Att det är sannolikt omöjligt att uppfylla informationsplikten eller att den avsevärt försvårar uppfyllandet av målen med behandlingen menar Artikel 29-arbetsgruppen torde vara sällan förekommande. Skulle emellertid den situationen uppstå att den personuppgiftsansvarige saknar möjlighet att informera de registrerade, t.ex. att tredje part inte lämnat ut några kontaktuppgifter om de registrerade, är innebörden av ordalydelsen ”göra uppgifterna tillgängliga för allmänheten” enligt arbetsgruppen att denne åtminstone måste informerar om personuppgiftsbehandlingen på sin hemsida.[68]

Enligt art. 14.2 f dataskyddsförordningen ska den personuppgiftsansvarige uppge varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor. Ett annat hinder för att uppfylla denna informationsplikt kan vara att uppgifter härrör från flera olika källor. Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, anger skäl 61 att den personuppgiftsansvarige i stället lämnar allmän information om källorna.

Hur ska information om registreringen av personuppgifter i Embrace lämnas till berörda enskilda inom ramen för det lokala brottsförebyggande arbetet? När ska det ske? Och av vem?

Som redovisats ska information till den registrerade som huvudregel lämnas i skriftlig form. Men information får också lämnas ”i någon annan form, inbegripet, när så är lämpligt, i elektronisk form” (art. 21.1). Artikel 29-arbetsgruppen skriver i sin vägledning om informationsskyldighet att det är omständigheterna i det enskilda fallet som ska vara styrande för valet av form och sätt för informationen till en registrerad.[69] Några exempel på sätt att lämna information finns inte i dataskyddsförordningen. Däremot finns det rekommendationer från Artikel 29-arbetsgruppen. Bl.a. rekommenderar arbetsgruppen att om den personuppgiftsansvarige har en hemsida på internet, information om dennes personuppgiftsbehandling bör publiceras där, t.ex. i form av en dataskyddspolicy eller i en annan form som tydligt visar att det handlar om information enligt art. 13 och/eller 14.[70] Arbetsgruppen rekommenderar också att en personuppgiftsansvarig prövar sig fram för att hitta ett sätt att nå fram med sin information om en viss typ av personuppgiftsbehandling.[71]

När information samlas in från den registrerade själv ska information lämnas ”när personuppgifterna erhålls” (art. 13.1). När uppgifter samlas in från en tredje part, vilket kan förväntas vara det vanliga fallet beträffande insamling om uppgifter i

[68] Ib. s. 26.
[69] Ib. s. 11.
[70] Ib. s. 13. Arbetsgruppen skriver: ”As noted above at paragraph 14, WP29 recommends that where a data controller has an online presence, an online layered privacy statement/ notice should be provided.”
[71] Ib.

Embrace avseende otrygghetsskapande händelser ute på ”fältet”, t.ex. en fastighetsskötare som lämnar uppgifter om skadegörelse på en hyresbostad med flera hyresgäster, ska informationen lämnas inom en månad till den registrerade.

Både art. 13 och 14 lägger en skyldighet på den personuppgiftsansvarige att tillhandahålla vederbörlig information till den registrerade (”...ska den personuppgiftsansvarige… till den registrerade lämna information…”). Det innebär enligt Artikel 29-arbetsgruppen att den personuppgiftsansvarige måste ta aktiva steg för att förmedla informationen till den registrerade. Det är inte den registrerade som ska ta initiativ till att få vederbörlig information.[72] Det krävs således någon form av aktivt handlande av den personuppgiftsansvarige för att säkerställa att den registrerade får del av informationen. Art. 13 och 14 lägger inte bara en skyldighet på den personuppgiftsansvarige att uppfylla sin informationsplikt när personuppgifter samlas in eller registreras utan också att tillmötesgå en begäran från registrerad om att få information om en viss typ av personuppgiftsbehandling. Den registrerade kan även tänkas utöva flera andra rättigheter, t.ex. att utfå ett registerutdrag (art. 15). Det måste således finnas rutiner på plats för att tillmötesgå enskilda som vill utöva sina rättigheter (se avsnitt 9.3).

Motsvarande bestämmelser om information finns i 4 kap. i brottsdatalagen, som bl.a. polisen ska iaktta fr.o.m. den 1 januari 2019 (tills vidare ska polisen beakta bestämmelserna om information till registrerade i 23 § respektive 25 – 27 §§ i den upphävda personuppgiftslagen, som dock alltjämt gäller för polisen t.o.m. 31 december 2018.

Enligt 4 kap. 5 § brottsdatalagen gäller inte informationsskyldigheten i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. annans fri- och rättigheter skyddas.

Om något av dessa undantag är uppfyllda, är den personuppgiftsansvarige inte heller skyldig att lämna ut skälen för beslut eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 4 kap. 9 eller 10 § brottsdatalagen.

Undantagen från informationsskyldigheten enligt första och andra styckena gäller även för en personuppgiftsansvarig som inte är en myndighet i motsvarande fall som avses i offentlighets- och sekretesslagen (2009:400).

Som framhållits aktualiseras behandling av personuppgifter i Embrace främst när gatu- och fastighetsadresser registreras av användare i tjänsten. Registrering av en brottsrelaterad eller otrygghetsskapande händelse som sker på en allmän plats, t.ex. ett torg eller en järnvägsstation, kan svårligen kopplas till enskilda fysiska personer.

---

[72] Ib. s. 16.

Det är alltså när gatu- och fastighetsadresser registreras om en händelse som informationsskyldigheten inträder.

Utgångspunkten enligt dataskyddsförordningen är att den personuppgiftsansvarige, t.ex. ett fastighets- eller bostadsbolag, ska lämna skriftlig information till de personer, t.ex. hyresgäster, vars fastighet eller vars egendom har utsatts för brott eller annan otrygghetsskapande händelse och informera vederbörande om att händelsen registreras i Embrace. Det gäller givetvis även den hyresgäst som eventuellt rapporterat händelsen. I sådana fall ska information lämnas till uppgiftslämnaren ”när personuppgifterna erhålls”. Det skulle kunna ske genom ett informationsblad som överlämnas på stället vid rapporteringstillfället. Övriga boende skulle kunna informeras genom ett anslag i trappuppgången om registreringen av händelsen i Embrace.

Det finns dock nackdelar med att informera hyresgäster och boende skriftligen när uppgifter om en händelse samlas in på fältet. Dels kan det kräva betydande arbetsinsatser för större fastighets- eller bostadsföretag. Dels finns en risk att fastighets- och bostadsbolaget missar att informera de boende i mängden av ärenden. Dels kan skriftlig information på platsen, dvs. information till samtliga boende på den adress där man registrerar en otrygghetsskapande händelse, såsom exempelvis misstanke om droghandel, väcka otrygghet snarare än trygghet hos de boende. Informationen skulle dessutom kunna misstänkliggöra alla hyresgäster. Som framhållits får en privat aktör, t.ex. ett fastighets- eller bostadsföretag, inte registrera några uppgifter om brott andra än uppgifter om brottsoffer (se avsitt 8.8).

I detta fall skulle informationen kunna leda till missförstånd hos de boende om att de registreras som brottslingar och föranleda att de motsätter sig personuppgiftsbehandlingen enligt art. 21.1. Det skulle därmed föreligga en situation där informationsskyldigheten enligt huvudregeln (skriftlig information…när personuppgifterna erhålls) avsevärt försvårar uppfyllandet av målen med behandlingen i Embrace enligt art. 14.5 b.

Enligt art. 12.1 får information i stället för skriftligen lämnas i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Vidare får den personuppgiftsansvarige underlåta att ge skriftlig information när personuppgifterna erhålls, eller när de erhålls från en tredje part, om den registrerade redan förfogar över informationen om personuppgiftsbehandlingen och vem som behandlar dennes personuppgifter.

Det sagda innebär att en kommun eller ett fastighets- eller bostadsföretag i stället skulle kunna informera om personuppgiftsbehandlingen på andra sätt genom etablerade kommunikationskanaler med invånare och hyresgäster. Det skulle kunna ske genom t.ex. nyhetsbrev som följer med fakturan för hyra, via e-postutskick, annonsering i lokaltidning i kombination med information på hemsidan. Det centrala är att informationen når samtliga som kan komma att beröras av registreringen. För ett bostadsbolag handlar det alltså om att informera samtliga boende om detta arbete och att om något händer så kommer det att registreras och att deras adress kan komma att registreras.

Informationen behöver inte vara uttömmande i sådana utskick. Däremot ska det på kommunens eller fastighets- eller bostadsföretagets sida finnas uttömmande information som uppfyller kraven i art. 13 och 14 i dataskyddsförordningen, till vilken information e-postmeddelandet eller nyhetsbrevet hänvisar, t.ex. medelst en länk.

Det är viktigt att bostadsföretaget då har dokumenterade rutiner för detta och att exempelvis nyinflyttade personer nås av informationen. Om något betydande förändras angående vad som registreras så ska ny information ges till de boende.

Genom sådana massiva och riktade regelbundna informationskampanjer kan den personuppgiftsansvarige underlåta att ge information på plats till boende m.fl. vid registrering av en otrygghetsskapande händelse eller ett brott eftersom berörda registrerade redan förfogar över information om personuppgiftsbehandlingen.

Informationsskyldigheten enligt dataskyddsförordningen omfattar både kommuner och organisationer inom näringslivet som använder Embrace. I brottsdatalagen, som polisen ska beakta när den använder Embrace, finns inte de undantag i dataskyddsförordningen som redovisas ovan utan flertalet andra som ska beaktas av polisen. I nuläget ska Polismyndigheten dock beakta bestämmelserna om information till registrerade i 23 § och 25 – 27 §§ i personuppgiftslagen, t.o.m. den 31 december 2018.

Polismyndigheten har idag ingen skyldighet att lämna information om sin personuppgiftsbehandling om uppgifterna samlats in från en annan källa än den registrerade. Samlas däremot uppgifter in från den registrerade själv ska information lämnas av polisen om personuppgiftsbehandlingen. Information behöver dock inte lämnas vid behandling som består av insamling av personuppgifter genom bilder eller ljud. Sådan information behöver inte heller lämnas om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen (2 kap. 2 § polisdatalagen).

Information till allmänheten om Polismyndighetens behandling av personuppgifter finns på myndighetens hemsida, https://polisen.se/Lagar-och-regler/Personuppgiftsbehandlingar/. På hemsidan finns även en blankett för enskilda för att erhålla information om de uppgifter som polisen behandlar om denne, s.k. registerutdrag. På hemsidan nämns exempel på personregister som polisen förfogar över.

För Polismyndighetens del medför t.ex. import av uppgifter från det system som registrerar brottsanmälningar (RAR) till Embrace inga förändringar i informationsskyldigheten. Embrace är ett register av flera som polisen förfogar över med stöd av polisdatalagen, och som polisen idag har lämnat information om på sin hemsida.

Som erinrats tidigare träder en ny lag om polisens behandling av personuppgifter inom brottsdatalagens område i kraft den 1 januari 2019. Den lagen innehåller inga bestämmelser om informationsskyldighet utan i stället gäller brottsdatalagens bestämmelser om information.

9.2 Personuppgiftsansvarigas skyldigheter

Personuppgiftsansvariga för Embrace, t.ex. kommuner, polisen och fastighets- och bostadsbolag, har ett flertal skyldigheter enligt dataskyddsförordningen respektive brottsdatalagen. Här berörs kort några av den personuppgiftsansvariges skyldigheter enligt dataskyddsförordningen respektive brottsdatalagen.

- Föra en förteckning över kategorier av personuppgiftsbehandlingar
- Rapportera personuppgiftsincidenter till Datainspektionen
- Rutiner för att omhänderta krav från den registrerade avseende olika rättigheter
- Skydda personuppgifter
- Iaktta privacy by design och privacy by default

Enligt art. 34.1 dataskyddsförordningen ska, om en personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten. Såvitt kan bedömas, mot bakgrund av att Embrace inte innehåller några individuppgifter, finns ingen sådan hög risk för enskildas fri- och rättigheter vid en incident, t.ex. ett dataintrång.

9.3 Den registrerade rättigheter

Den registrerade har åtta rättigheter, inklusive rätten till information (ovan) i dataskyddsförordningen som kan åberopas mot personuppgiftsansvariga. Beträffande Embrace kan den registrerade t.ex. åberopa rätten till rättelse, registerutdrag och begränsning av personuppgiftsbehandlingen oavsett om polisen, kommun eller en privat aktör behandlar personuppgifterna.

När polisen behandlar personuppgifter kan den registrerade med stöd av brottsdatalagen därutöver begära att Datainspektionen ska kontrollera personuppgiftsbehandlingen.

När kommun behandlar personuppgifter kan den registrerade inte åberopa rätten till att bli bortglömd (art. 17.3 b dataskyddsförordningen). Den registrerade får däremot när som helst göra invändningar mot (motsätta sig) behandling av personuppgifter (art. 21.1 dataskyddsförordningen). I sådant fall får kommunen inte längre behandla personuppgifterna, såvida den inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk. Det är oklart vad som menas med ”tvingande berättigade skäl”. Vad som närmast skulle kunna utgöra sådana skäl är en författningsreglerad skyldighet att bedriva brottsförebyggande arbete. En sådan skyldighet finns inte idag. Enligt art. 17.1 c har en registrerad rätt att bli bortglömd om den registrerade invänder mot (motsätter sig) behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre, eller den registrerade invänder mot behandlingen i enlighet med artikel 21.2. Det är oklart om denna rätt att bli bortglömd avser enbart

den lagliga grunden ”intresseavvägning” enligt art. 6.1. f eller om den även rymmer art. 6.1 e (arbetsuppgifter av allmänt intresse/myndighetsutövning). Rätten att göra invändning enligt art. 21.1 omfattar både punkten e och f i art. 6.1. Rättspraxis får utvisa vad som gäller. Övervägande skäl talar dock för att art. 17.1 c enbart kan åberopas när den lagliga grunden är ”intresseavvägning” (art. 6.1 f), varför den registrerade –enligt denna tolkning – inte kan begära att bli raderad ur Embrace vid en invändning.

Om en privat aktör behandlar personuppgifter kan den registrerad enligt dataskyddsförordningen invända mot personuppgiftsbehandlingen (motsätta sig) enligt art. 21.1 samt rätten att bli bortglömd enligt art. 17.1 c (se ovan), om han eller hon samtidigt har gjort en invändning mot personuppgiftsbehandlingen. Det finns ett flertal undantag från rättigheten att bli bortglömd som kan bli tillämpliga i vissa fall.

Däremot kan den enskilde inte åberopa rätten till dataportabilitet mot någon av nämnda aktörer. Dataportabilitet innebär en rätt för den registrerade att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta (art. 20).

9.4 Embrace Safetys skyldigheter

Embrace Safety avser att tillhandahålla tjänsten Embrace som en molntjänst samt i rollen som personuppgiftsbiträde.

I den rollen har Embrace Safety ett par skyldigheter enligt dataskyddsförordningen respektive brottsdatalagen. Bl.a. ska bolaget

- Säkerställa skyddet för personuppgifterna i tjänsten
- Följa de instruktioner som meddelas i ett skriftligt avtal med den personuppgiftsansvarige
- Rapportera personuppgiftsincidenter utan dröjsmål till den personuppgiftsansvarige, och
- Föra ett register för kategorier av personuppgiftsbehandlingar och kunder.

På Örebro Universitet Enterprise AB:s uppdrag

Manólis Nymark

1 Några centrala begrepp i utredningen

I det följande lämnas en redogörelse för några centrala begrepp i utredningen samt gällande rätt för aktuella frågeställningar.

1.1 Behandling

Med behandling av personuppgifter avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

1.2 Personuppgifter

Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

1.3 Personuppgiftsansvarig

Med personuppgiftsansvarig avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

1.4 Personuppgiftsbiträde

Med personuppgiftsbiträde avses den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

1.5 Registrerad

Med registrerad avses den som personuppgiften avser.

1.6 Sekretess

Med sekretess avses bestämmelser i offentlighets- och sekretesslagen (2009:400), förkortad OSL, om förbud att röja uppgifter. Bestämmelserna ska beaktas av statliga och kommunala myndigheter samt aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där en kommun eller ett landsting utövar ett rättsligt bestämmande inflytande. Med sekretess avses förbud att röja uppgift, vare sig detta sker muntligen, genom utlämnande av allmän handling eller på något annat sätt.

1.7 Sekretessbrytande bestämmelse

Med sekretessbrytande bestämmelse avses en bestämmelse som säger att en myndighet *får* lämna ut en sekretessbelagd uppgift under vissa förutsättningar utan att behöva göra en menprövning eller inhämta ett samtycke från den invånare som uppgiften berör.

1.8 Uppgiftsskyldighet

Med uppgiftsskyldighet avses en bestämmelse som säger att en myndighet *ska* lämna ut en sekretessbelagd uppgift under vissa förutsättningar utan att behöva göra en menprövning eller inhämta ett samtycke från den invånare som uppgiften berör.