Finalitetsprincipen försvårar en effektiv brottsbekämpning

Sofie Lindblom

Tillgång till information är avgörande för att bekämpa den organiserade brottsligheten

Samhällsutvecklingen har inte varit positiv sedan dataskyddsreformen beslutades 2016. Under de senaste åren har våld i form av skjutningar och sprängningar ökat. Personer inom kriminella nätverk begår våldsbrott samtidigt som de använder sig av komplicerade upplägg för penningtvätt och brott mot välfärdssystemen. Den organiserade brottsligheten har fått fäste i samhället på ett sätt som gör att den nu börjar benämnas systemhotande.

Flera statliga utredningar, myndigheter och andra aktörer har framfört att utökade möjligheter till informationsutbyte är nödvändigt för att kunna bekämpa brott och för att myndigheterna ska kunna skydda sina verksamheter och därmed det allmänna. Tillgång till information är avgörande för att bekämpa den organiserade brottsligheten, inte bara för brottsbekämpande myndigheter. För att brottsfenomen ska kunna upptäckas och sårbarheter täppas till behöver också exempelvis de myndigheter som ansvarar för välfärds- och skattesystemen och andra system som används i avancerade brottsupplägg kunna utbyta information med varandra. Det är också samhällsekonomiskt mest effektivt om den information som en aktör samlar in kan användas av flera, t.ex. vid kamerabevakning, i stället för att samma information ska samlas in av flera genom att alla sätter upp egna kameror. Ett effektivt och ändamålsenligt informationsutbyte är därför centralt, ytterst för att upprätthålla förtroendet för den offentliga förvaltningen och för att skydda statsfinanserna. Det är också en förutsättning för en effektiv brottsbekämpning.

Regeringen har uttalat att sekretessgränserna mellan myndigheter ska rivas och flera utredningar har i uppdrag att titta på hur informationsutbyte mellan myndigheter kan underlättas. Den information som myndigheter behöver utbyta innehåller ofta personuppgifter. Att riva

sekretessgränser eller förenkla sekretessregelverket är därför inte tillräckligt. Det krävs också att en myndighet är skyldig eller i vart fall har rätt att behandla personuppgifter för att lämna ut dem till andra för att informationsutbyte ska komma till stånd. Även här krävs en enkel reglering. En viktig fråga är därför om dataskyddsregelverket medger informationsutbyte i den utsträckning som krävs för en effektiv brottsbekämpning. Denna artikel fokuserar på om regelverket som styr utlämnande av uppgifter till andra är ändamålsenligt. Frågan om dataskyddsregelverket också ger tillräckliga möjligheter för den mottagande myndigheten att behandla och lagra uppgifterna tas inte upp här, även om den är minst lika viktig.

Syftet avgör vilket regelverk som är tillämpligt

Att lämna information till en annan myndighet innebär en vidarebehandling av de personuppgifter som redan behandlas, vilket ofta innebär att uppgifterna behandlas för nya ändamål. Regleringen av när personuppgifter får behandlas för nya ändamål skiljer sig mellan de två huvudsakliga regelverken på dataskyddsområdet, dataskyddsförordningen och brottsdatalagen. Det finns därför skäl att först titta på tillämpningsområdet för de båda regelverken.

Dataskyddsförordningen gäller för all personuppgiftsbehandling som omfattas av unionsrätten, om inte dataskyddsdirektivet är tillämpligt. Dataskyddsdirektivet har i svensk rätt genomförts genom brottsdatalagen (2018:1177) med tillhörande förordning. Det innebär att gränsen mellan när de olika regelverken ska tillämpas regleras i brottsdatalagen.

Brottsdatalagen gäller för behöriga myndigheter 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. Det är huvudsakligen myndigheterna i rättskedjan som är behöriga myndigheter, men lagen gäller även andra som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. I lagen räknas inte de behöriga myndigheterna upp, eftersom lagen enbart gäller när behöriga myndigheter behandlar personuppgifter för de i lagen angivna syftena. Det innebär att när dessa myndigheter eller organ behandlar personuppgifter för andra syften än dem som anges i brottsdatalagen ska de i stället tillämpa dataskyddsförordningen. Brottsdatalagen gäller inte när andra än behöriga myndigheter behand-

lar personuppgifter, även om behandlingen har ett brottsbekämpande syfte, t.ex. när en myndighet anmäler ett brott till Polismyndigheten.

Dataskyddsförordningen och brottsdatalagen kan vara tillämpliga parallellt om samma personuppgift behandlas för olika syften, men de kan aldrig tillämpas samtidigt på personuppgiftsbehandling som bara har ett syfte. Det är alltså i slutändan syftet med personuppgiftsbehandlingen som avgör vilket regelverk som är tillämpligt. Det gäller oavsett om det är första gången en uppgift behandlas eller om den ska behandlas för nya ändamål. När en uppgift ska behandlas för att lämnas ut till någon annan måste det därför alltid avgöras om det nya ändamålet med behandlingen omfattas av brottsdatalagens tillämpningsområde eller inte.

Regleringen av behandling för nya ändamål

Dataskyddsreformen har ändrat förutsättningarna

Möjligheterna att behandla insamlade personuppgifter för nya ändamål har sedan länge styrts av finalitetsprincipen, enligt vilken personuppgifter inte får behandlas på ett sätt som står i strid med insamlingsändamålet. Den reglerades tidigare i 9 § första stycket d personuppgiftslagen (1998:204) och kompletterades för de brottsbekämpande myndigheterna av s.k. sekundära ändamålsbestämmelser i deras registerförfattningar. I de sekundära ändamålsbestämmelserna reglerades när det var tillåtet att behandla personuppgifter som behandlades i myndighetens brottsbekämpande verksamhet för att tillhandahålla information till andra myndigheter eller till andra verksamheter inom den egna myndigheten för deras behov.

Efter dataskyddsreformen gäller det att hålla tungan rätt i mun, för regleringen av behandling för nya ändamål ser olika ut beroende på vilket regelverk som är tillämpligt på den ursprungliga behandlingen och på behandlingen för det nya ändamålet. Här finns tre olika scenarier:

- Personuppgifter som behandlas med stöd av brottsdatalagen ska behandlas för ett ändamål som ligger inom brottsdatalagens tillämpningsområde.
- Personuppgifter som behandlas med stöd av brottsdatalagen ska behandlas för ett ändamål som ligger inom dataskyddsförordningens tillämpningsområde.
- Personuppgifter som behandlas med stöd av dataskyddsförordningen ska behandlas för ett nytt ändamål.

Personuppgifter som behandlas med stöd av brottsdatalagen ska behandlas för ett ändamål som ligger inom brottsdatalagens tillämpningsområde

I artikel 4.1.b i dataskyddsdirektivet regleras finalitetsprincipen. Samtidigt framgår det i artikel 4.2 att behandling för andra ändamål inom direktivets tillämpningsområde än det för vilket uppgifter samlades in ska tillåtas, om den personuppgiftsansvarige enligt unionsrätten eller nationell rätt får behandla personuppgifter för ett sådant ändamål och behandlingen är nödvändig och står i proportion till det andra ändamålet. I förarbetena till brottsdatalagen konstateras att det måste innebära att all behandling för ändamål som ligger inom direktivets tillämpningsområde ska anses förenlig med insamlingsändamålen, under förutsättning att behandlingen är nödvändig och står i proportion till det nya ändamålet. Det konstateras vidare att det alltså saknar betydelse om det är den personuppgiftsansvarige som ursprungligen samlat in personuppgifterna som behandlar uppgifterna för det nya ändamålet eller om det är en annan personuppgiftsansvarig, så länge de båda är behöriga myndigheter och behandlingen ligger inom direktivets tillämpningsområde (prop. 2017/18:232 s. 126). Även behandling för att lämna ut personuppgifter till någon som inte är en behörig myndighet kan omfattas av direktivet, om ändamålet för behandlingen ligger inom direktivets tillämpningsområde. Som exempel kan nämnas att Polismyndigheten vid utredningen av ett brott behöver skicka personuppgifter till en icke brottsbekämpande myndighet för att få information för utredningen av brottet.

Mot den bakgrunden regleras inte finalitetsprincipen i brottsdatalagen. Av 2 kap. 4 § första stycket brottsdatalagen framgår i stället att innan personuppgifter som behandlas med stöd av brottsdatalagen får behandlas för ett nytt ändamål inom lagens tillämpningsområde, ska det säkerställas att det finns en rättslig grund för den nya behandlingen och att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. Enligt andra stycket ska någon prövning inte göras om det finns en författningsreglerad uppgiftsskyldighet.

Personuppgifter som behandlas med stöd av brottsdatalagen ska behandlas för ett ändamål som ligger inom dataskyddsförordningens tillämpningsområde

I artikel 9 i dataskyddsdirektivet regleras vad som gäller när personuppgifter som behandlas med stöd av direktivet ska behandlas för ändamål utanför direktivets tillämpningsområde, t.ex. för att lämnas ut till

myndigheter och andra aktörer som inte är behöriga myndigheter för deras behov. Av artikeln framgår att sådan behandling endast får ske om behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt och att dataskyddsförordningen då ska tillämpas. I förarbetena till brottsdatalagen konstateras med hänvisning till skäl 34 till direktivet att dataskyddsförordningen är tillämplig redan på behöriga myndigheters behandling för att tillhandahålla personuppgifter till andra myndigheter, om ändamålet ligger utanför brottsdatalagens tillämpningsområde. Det innebär att prövningen av om en sådan behandling är tillåten ska göras enbart med utgångspunkt i bestämmelserna i dataskyddsförordningen (prop. 2017/18:232 s. 131 f.). Behandlingen måste vila på en rättslig grund. De rättsliga grunderna räknas uttömmande upp i artikel 6.1 i förordningen. När behöriga myndigheter lämnar ut personuppgifter utanför brottsdatalagens tillämpningsområde är det framför allt punkterna c (behandlingen är nödvändig för att fullgöra en rättslig förpliktelse), d (behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller annan fysisk person) eller e (behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning) som blir aktuella.

Eftersom behandlingen för ett nytt ändamål som inte omfattas av brottsdatalagen blir en första behandling enligt dataskyddsförordningen är det inte fråga om vidarebehandling enligt något av regelverken, vilket gör att finalitetsprincipen inte ska tillämpas på behandlingen. Innan personuppgifter som behandlas med stöd av brottsdatalagen behandlas för ändamål utanför lagens tillämpningsområde ska det enligt 2 kap. 22 § brottsdatalagen dock säkerställas att det är nödvändigt och proportionerligt att uppgifterna behandlas för det nya ändamålet. Enligt andra stycket ska någon prövning inte göras om det finns en författningsreglerad uppgiftsskyldighet.

Personuppgifter som behandlas med stöd av dataskyddsförordningen ska behandlas för ett nytt ändamål

Artiklarna 5 och 6 i dataskyddsförordningen är grundläggande vid behandling av personuppgifter enligt förordningen och ska tillämpas kumulativt. I artikel 6 slås fast att en personuppgiftsbehandling är laglig endast om det går att stödja den på någon av de rättsliga grunder som framgår av bestämmelsen. I artikel 5 finns ett antal grundläggande principer som gäller vid all behandling av personuppgifter enligt förordningen. En viktig princip är principen om ändamålsbegränsning. Principen består av två delar, principen om ändamålsbestämning och

finalitetsprincipen. I detta sammanhang är det finalitetsprincipen som är av intresse.

I artikel 6.4 i dataskyddsförordningen anges de kriterier som den personuppgiftsansvarige måste beakta för att fastställa om behandling för nya ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in (det s.k. förenlighetstestet). Enligt bestämmelsen ska den personuppgiftsansvarige bland annat beakta:

- kopplingar som finns mellan insamlingsändamålen och ändamålet för den avsedda ytterligare behandlingen
- det sammanhang inom vilket personuppgifterna samlats in
- personuppgifternas art
- eventuella konsekvenser för den registrerade av den fortsatta behandlingen och
- förekomsten av lämpliga skyddsåtgärder.

I skäl 50 i dataskyddsförordningen anges uttryckligen att den personuppgiftsansvarige särskilt bör beakta de registrerades rimliga förväntningar på hur deras uppgifter kommer att användas. Där framgår också att om en vidarebehandling är förenlig med det ursprungliga ändamålet krävs det inte någon separat rättslig grund för vidarebehandlingen. Den personuppgiftsansvarige kan således stödja sig på samma rättsliga grund som användes som stöd för att samla in personuppgifterna. Artikel-29 gruppen har uttalat att det finns utrymme för en viss flexibilitet vid tillämpningen av reglerna om vidarebehandling och att behandling som sker efter ett insamlande inte direkt måste motsvaras av ett från början angivet ändamål, exempelvis där förväntningar från samhället eller från de registrerade ändras över tid (Artikel-29 gruppens yttrande 03/2013, s. 21).

I vissa situationer är vidarebehandling tillåten utan att den personuppgiftsansvarige först gör ett förenlighetstest. Av artikel 6.4 i dataskyddsförordningen framgår nämligen att en vidarebehandling är tillåten om den grundar sig på den registrerades samtycke eller på unionsrätten eller en medlemsstats nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda vissa specifika mål, t.ex. förebyggande, utredning eller lagföring av brott. Medlemsstaterna har alltså möjlighet att införa mer generella undantag som tillåter utlämnande av personuppgifter i ett brottsbekämpande syfte. Något sådant generellt undantag finns inte i Sverige.

Medger regleringen ett effektivt informationsutbyte?

Vilka slutsatser kan man dra av detta? För det första kan det konstateras att finalitetsprincipen aldrig blir tillämplig när personuppgifter som behandlas med stöd av brottsdatalagen ska behandlas för nya ändamål. Oavsett vilket regelverk som är tillämpligt på behandlingen för det nya ändamålet krävs att det finns en rättslig grund för behandlingen för det nya ändamålet, antingen i brottsdatalagen eller i dataskyddsförordningen, och att det är nödvändigt och proportionerligt att behandla uppgifterna för det nya ändamålet. Regleringen är förhållandevis enkel att tillämpa och följer dessutom av EU-rätten, varför det inte finns möjlighet till några förändringar eller förtydliganden i den här delen.

När det däremot gäller personuppgifter som behandlas enligt dataskyddsförordningen är regleringen mer svårtillämpad. Vid behandling för nya ändamål gäller finalitetsprincipen och det måste säkerställas att behandlingen för det nya ändamålet inte är oförenlig med ändamålet för den ursprungliga behandlingen, vilket inte alltid är det lättaste. Myndigheter och andra aktörer drar sig ofta för att lämna uppgifter till brottsbekämpande myndigheter eller till varandra av rädsla för att åläggas sanktionsavgifter om de gör fel. Det finns också de som anser att det vid en bedömning enligt förenlighetstestet i normalfallet inte finns förutsättningar att lämna ut personuppgifter till en brottsbekämpande myndighet, eftersom den personuppgiftsansvarige sällan tillräckligt tydligt har angett att ett sådant överlämnande kan komma att ske i samband med insamlingstillfället. Finalitetsprincipen försvårar därmed en effektiv brottsbekämpning.

Vad kan göras för att förenkla regleringen?

En otillfredsställande situation

Att det råder tveksamhet kring om det är tillåtet att lämna ut uppgifter till brottsbekämpande myndigheter eller till andra myndigheter i ett brottsbekämpande syfte är inte tillfredsställande i en tid där tillgång till information är det avgörande verktyget i kampen mot den organiserade brottsligheten. Går det att göra något för att förenkla regleringen som styr utbyte av personuppgifter som behandlas med stöd av dataskyddsförordningen?

Det finns flera vägar att gå. Fler myndigheter kan ges ett brottsbekämpande uppdrag och det kan införas uppgiftsskyldigheter i större utsträckning. Man kan också förenkla prövningen som ska göras när uppgifter ska behandlas för nya ändamål enligt dataskyddsförordningen.

Bör fler myndigheter ges ett brottsbekämpande uppdrag?

Det har under flera år påtalats att fler myndigheter och andra aktörer måste engagera sig i brottsbekämpningen om det ska gå att vända utvecklingen. De ska inte bara göra vad de kan för att förebygga att brott begås inom sina respektive verksamheter, utan måste också överväga vad de kan bidra med för att förebygga brott även i annan verksamhet. Det innebär att de behöver behandla personuppgifter i brottsbekämpande syfte. Innebär det att de då ska tillämpa brottsdatalagen?

Brottsdatalagen blir tillämplig bara när det är behöriga myndigheter som behandlar personuppgifter i brottsbekämpande syfte. En myndighet är behörig myndighet om den har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Det är inte tillräckligt att myndigheten har en skyldighet att anmäla brott eller någon annan skyldighet att lämna uppgifter till brottsbekämpande myndigheter, utan det krävs konkreta uppgifter i brottsbekämpningen, t.ex. när Justitiekanslern agerar i egenskap av åklagare i mål om tryckfrihetsbrott (se prop. 2017/18:232 s. 429 f.). För att en myndighet ska omfattas av brottsdatalagens tillämpningsområde krävs alltså att den ges ett tydligt brottsbekämpande uppdrag.

Lagen (2023:196) om kommuners ansvar för brottsförebyggande arbete, som trädde i kraft i juli 2023, är ett färskt exempel på att lagstiftaren kan välja att reglera ett brottsbekämpande uppdrag för att det brottsförebyggande arbetet inte har prioriterats tillräckligt. I förarbetena till lagen konstateras att kommunerna har en särskilt viktig roll i samhällets samlade brottsförebyggande arbete och att det finns utrymme att utveckla och intensifiera det arbete som bedrivs av kommunerna, varför kommunernas ansvar för brottsförebyggande arbete ska regleras (prop. 2022/23:43 s. 14 f.). Kommunen ska enligt lagen ta fram en lägesbild över brottsligheten i kommunen. Med lägesbilden som underlag ska kommunen ta fram en plan för vilka åtgärder kommunen avser att vidta för att förebygga brott. Det är enligt min mening tillräckligt konkreta arbetsuppgifter för att kommunerna i den delen ska betraktas som behörig myndighet i brottsdatalagens mening.

Brottsdatalagen är mer tillåtande än vad dataskyddsförordningen är, exempelvis när det gäller möjligheterna att behandla känsliga personuppgifter och att behandla uppgifter för nya ändamål inom lagens tillämpningsområde. Även om fler myndigheter engagerar sig i brottsbekämpningen och börjar behandla personuppgifter i brottsbekämpande syfte, är det inte rimligt att de alla ges ett brottsbekämpande uppdrag så att de blir behöriga myndigheter enligt brottsdatalagen. Det skulle föra för långt att utsträcka kretsen behöriga myndigheter till alla

som behöver engagera sig i brottsbekämpning. Det finns dock ytterligare några myndigheter som har en sådan central roll för en effektiv brottsbekämpning att de borde ges ett brottsbekämpande uppdrag och bli behöriga myndigheter i brottsdatalagens mening.

Det tydligaste exemplet är Utbetalningsmyndigheten, som ska inrättas den 1 januari 2024. I budgetpropositionen för 2022 anförde regeringen att arbetet mot felaktiga utbetalningar och brottslighet riktad mot välfärdssystemen bör stärkas ytterligare och att en ny myndighet för systemövergripande kontroller av utbetalningar från välfärdssystemen därför bör bildas (prop. 2021/22:1 utg.omr. 2 avsnitt 6). Den nya myndighetens uppdrag ska vara att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen (dir. 2022:8 s. 2). Det är dock myndigheten från vilken informationen kommer som ska ansvara för att anmäla eventuella brott som upptäcks till brottsbekämpande myndigheter. Varför då? Den nya myndigheten kommer ha överblick över alla utbetalningar som görs och därigenom ha en unik möjlighet att upptäcka och täppa till de strukturella sårbarheter i systemen som utnyttjas av kriminella. Enligt min mening är det givet att den myndighet som har överblicken och som har i uppdrag att förebygga, förhindra och upptäcka felaktiga utbetalningar också ska ha till uppgift att förebygga, förhindra och upptäcka brott i de system som myndigheten är satt att kontrollera.

Andra myndigheter som har en viktig roll i att förhindra den kriminella ekonomin från att växa och som kanske borde ges ett brottsbekämpande uppdrag är Bolagsverket, den del av Skatteverket som ansvarar för folkbokföringen, Transportstyrelsen, Finansinspektionen och Inspektionen för vård och omsorg.

Bör det införas uppgiftsskyldighet i fler fall?

Högsta förvaltningsdomstolen har i mål 433-20 prövat frågan om uppgiftsskyldigheten mellan myndigheter enligt 6 kap. 5 § offentlighets- och sekretesslagen (2009:400) är förenlig med finalitetsprincipen. Domstolen konstaterar att uppgiftsskyldigheten förutsätter att endast uppgifter som inte omfattas av sekretess lämnas och att lagstiftaren därigenom får anses ha tagit ställning till att ett uppgiftslämnande inte är oförenligt med det eller de ändamål för vilket uppgifterna samlades in. Utöver sekretessprövningen ska en myndighet således inte göra någon kontroll av förenligheten med finalitetsprincipen i samband med lämnande av uppgifter enligt 6 kap. 5 § offentlighets- och sekretesslagen. Samma resonemang bör kunna föras när det gäller annan uppgiftsskyldighet, eftersom en sådan skyldighet förutsätter att uppgifterna som ska lämnas

ut inte omfattas av sekretess eller att det finns en tillämplig sekretessbrytande bestämmelse. En möjlighet att förenkla informationsutbyte är därför att införa fler uppgiftsskyldigheter, exempelvis när en myndighet har ett ofta återkommande behov av personuppgifter som behandlas av en annan myndighet med stöd av dataskyddsförordningen.

En förenklad prövning vid behandling för nya ändamål enligt dataskyddsförordningen

Även om ytterligare några myndigheter skulle ges ett brottsbekämpande uppdrag och det skulle införas uppgiftsskyldighet i de fall där det finns ett ofta återkommande behov av information skulle det långt ifrån tillgodose alla behov av att utbyta information. Det som skulle få störst effekt är att förenkla prövningen av när personuppgifter får behandlas för nya ändamål enligt dataskyddsförordningen och att skapa ett tydligt stöd för att lämna ut uppgifter i ett brottsbekämpande syfte.

Ett förslag till lösning

Som nämnts tidigare finns det i artikel 6.4 i förordningen möjlighet att införa mer generella undantag från finalitetsprincipen som tillåter utlämnande av personuppgifter i ett brottsbekämpande syfte, om det är nödvändigt och proportionerligt i ett demokratiskt samhälle. Bestämmelsen är formulerad på ett likartat sätt som artikel 9 i dataskyddsdirektivet, som reglerar behandling för nya ändamål inom direktivets tillämpningsområde. Man skulle därför kunna införa ett generellt undantag från finalitetsprincipen och förenlighetstestet som motsvarar vad som gäller enligt brottsdatalagen, nämligen att det är nödvändigt och proportionerligt att behandla personuppgifterna för det nya ändamålet. En sådan bestämmelse skulle kunna tas in i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Undantaget bör gälla behandling för nya ändamål som har ett brottsbekämpande syfte. Det bör inte bara gälla information som lämnas till en brottskämpande myndighet, utan även träffa myndigheter som inte har ett uttryckligt brottsbekämpande uppdrag men som måste tänka brottsbekämpning i sin verksamhet, t.ex. myndigheterna som ansvarar för välfärdssystemen. Bestämmelsen skulle motsvara de tidigare s.k. sekundära ändamålsbestämmelserna som angav när det var tillåtet att tillhandahålla information till andra för deras behov. På samma sätt som enligt de sekundära ändamålsbestämmelserna skulle tillämparen med den nya bestämmelsen endast behöva avgöra om det finns en rättslig

grund för behandlingen och om det är nödvändigt och proportionerligt att lämna informationen som behövs i en annan myndighets verksamhet för brottsbekämpande syften. Någon bedömning av om utlämnandet är förenligt med det ursprungliga ändamålet med personuppgiftsbehandlingen skulle inte behövas.

Att ersätta finalitetsprincipen och förenlighetstestet med en prövning av nödvändighet och proportionalitet skulle göra utbyte av personuppgifter i brottsbekämpande syfte betydligt enklare. Ett sådant tydliggörande av att det på dataskyddsförordningens område är tillåtet att lämna ut uppgifter för brottsbekämpande ändamål skulle få stor effekt i brottsbekämpningen genom att fler skulle våga, och kunna, dela med sig av den information de har tillgång till.