Kommittédirektiv

Säkerhetspolisens informationshantering

Beslut vid regeringssammanträde den 11 maj 2023

Sammanfattning

En särskild utredare ska göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Syftet är att skapa ändamålsenliga regler som är anpassade efter dagens behov och möjligheter. Reglerna bör som utgångspunkt ge Säkerhetspolisen ökade möjligheter att behandla personuppgifter, särskilt vad gäller att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel.

Utredaren ska noga väga myndigheternas behov av att behandla personuppgifter mot den enskildes rätt till skydd för sin personliga integritet. I uppdraget ingår att lämna nödvändiga författningsförslag.

Inom ramen för en översyn av regleringen ska utredaren bl.a.

- beskriva dagens rättsliga möjligheter för Säkerhetspolisen att behandla personuppgifter, särskilt vad gäller att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel,
- undersöka i vilken utsträckning dagens regelverk försvårar en effektiv informationshantering i Säkerhetspolisens verksamhet,
- lämna förslag som gör att information kan hanteras av Säkerhetspolisen på ett mer ändamålsenligt sätt än i dag, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 15 november 2024.

Varför behövs det en utredning?

Teknik- och samhällsutvecklingen kräver nya åtgärder

Till Säkerhetspolisens uppgifter hör bland annat att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott samt att utreda och beivra sådana brott.

Samhället står ständigt inför stora och föränderliga säkerhetsutmaningar. Hotbilden mot Sverige blir alltmer komplex och det ställer förändrade krav på Säkerhetspolisens förmåga. Digitaliseringen och den tekniska utvecklingen har förändrat samhället i grunden. Förändringen har inneburit att det produceras enorma mängder information. Digitalisering och teknikutveckling har också bidragit till att utveckla hotaktörernas förmåga. Enligt Säkerhetspolisen sker varje dag försök att stjäla uppgifter av betydelse för Sveriges säkerhet och försök att påverka svenskt beslutsfattande på olovliga sätt. Samtidigt bedrivs annan säkerhetshotande verksamhet riktad mot Sverige. Ett förstörande cyberangrepp från främmande makt kan få mycket allvarliga konsekvenser för Sveriges säkerhet och hota jobb, välfärd och konkurrenskraft. Angreppen kan också påverka våra grundläggande fri- och rättigheter, vårt politiska oberoende och vår territoriella suveränitet. Vidare har digitaliseringen gjort extremistmiljöerna globala och tillgängliga för många. Nya digitala plattformar ger förbättrade förutsättningar för kommunikation och möjligheter att hitta och påverka likasinnade.

De möjligheter som teknikutvecklingen innebär behöver tas tillvara också i Säkerhetspolisens arbete. Säkerhetspolisen arbetar ofta initialt utifrån ofullständig information. För att kunna upptäcka okända säkerhetshot måste Säkerhetspolisen samla in stora mängder information, som många gånger är helt öppen, för att analysera vilka uppgifter som kan vara relevanta att agera utifrån, exempelvis för att upptäcka spioneribrottslighet och förhindra terroristattentat. Säkerhetspolisen måste ha förutsättningar och förmåga att snabbt anpassa sig och utveckla nya metoder och lösningar. Myndighetens uppdrag att bedriva underrättelse- och säkerhetsarbete innebär att huvudfokus ligger på att förebygga, förhindra och upptäcka säkerhetshotande verksamhet. För att lösa uppdraget behöver myndigheten ha tillgång till relevant information och på ett effektivt sätt kunna hantera och bearbeta de stora informationsmängderna. Detta ställer nya krav på

Säkerhetspolisens arbetsmetoder och den lagstiftning som reglerar myndighetens informationshantering.

I egenskap av totalförsvarsmyndighet ska Säkerhetspolisen dessutom kunna fullgöra sitt uppdrag vid höjd beredskap och i krig. Det innebär att förutsättningarna för Säkerhetspolisens informationshantering även påverkar myndighetens möjligheter att utföra sina uppgifter inom totalförsvaret. Det försämrade säkerhetsläget i Europa efter Rysslands invasion av Ukraina och Sveriges Natoansökan har ytterligare tydliggjort behovet av att prioritera förmågan inom totalförsvaret. Säkerhetspolisens informationshantering är därför central även utifrån ett totalförsvarsperspektiv.

Stora informationsmängder kan hanteras med tekniska hjälpmedel

Säkerhetspolisen framhåller att det inte längre är möjligt att manuellt granska och strukturera uppgifter med hänsyn till den enorma mängden information som kan vara av intresse för myndighetens verksamhet. Med en sådan ordning kan endast en bråkdel av relevant information analyseras och bedömas. Till skillnad mot tidigare finns det i dag effektiv programvara som kan automatisera informationshanteringen och generera snabbare och mer träffsäkra resultat. Sådan programvara kan exempelvis göra en initial ytlig granskning av stora datamängder och flagga upp information som sannolikt är relevant. En manuell granskning behöver då endast göras av en mindre mängd information som har mer direkt relevans för Säkerhetspolisens uppdrag.

Dagens regelverk behöver ses över

Under 2016 enades EU om en genomgripande dataskyddsreform som skulle vara genomförd under våren 2018. Reformen omfattade dels dataskyddsförordningen ((EU) 2016/679), dels dataskyddsdirektivet ((EU) 2016/680). Dataskyddsdirektivet gäller behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

Dataskyddsdirektivet har i svensk rätt i huvudsak genomförts genom en ny ramlag, brottsdatalagen (2018:1177), som trädde i kraft den 1 augusti 2018. Verksamhet som rör nationell säkerhet omfattas däremot inte av unionsrätten. Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet omfattas alltså inte av dataskyddsdirektivet och har mot

den bakgrunden också undantagits från brottsdatalagens tillämpningsområde (1 kap. 4 § brottsdatalagen).

Jämfört med Polismyndigheten har Säkerhetspolisen en betydligt mer begränsad verksamhet, inriktad på några få områden. Tyngdpunkten ligger på att förebygga, förhindra och upptäcka brottslig verksamhet. Den brottsutredande verksamheten är mer begränsad. Säkerhetspolisen har i uppdrag att skydda Sveriges demokratiska system, medborgarnas fri- och rättigheter och den nationella säkerheten. Säkerhetspolisens verksamhet rör därmed i princip uteslutande nationell säkerhet. Den absoluta merparten av Säkerhetspolisens personuppgiftsbehandling ligger alltså utanför brottsdatalagens tillämpningsområde. I dessa fall gäller lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter (Säkerhetspolisens datalag) och förordningen (2019:1235) om Säkerhetspolisens behandling av personuppgifter. Trots de olikheter i fråga om myndigheternas verksamhet som nämns ovan har Säkerhetspolisens datalag utformats med brottsdatalagens systematik och innehåll som utgångspunkt.

Säkerhetspolisens datalag är visserligen ganska ny men många av bestämmelserna har överförts mer eller mindre oförändrade från tidigare lagstiftning. Det innebär att stora delar av det regelverk som påverkar möjligheterna att behandla personuppgifter kommer från en tid då inte bara hoten mot Sveriges säkerhet utan också de tekniska möjligheterna att behandla personuppgifter var annorlunda än i dag. Regelverket är alltså inte fullt ut anpassat till dagens förhållanden. Vidare står det klart att den tekniska utvecklingen har inneburit att det produceras enorma mängder information och att det samtidigt har skapats nya möjligheter för Säkerhetspolisen att med hjälp av automatiserade processer behandla stora informationsmängder. Det finns dock enligt nuvarande regelverk tydliga begränsningar för Säkerhetspolisens möjligheter att analysera stora datamängder med hjälp av tekniska hjälpmedel. Säkerhetspolisen anser att förbättrade möjligheter att hantera stora informationsmängder är en förutsättning för att myndigheten ska kunna lösa sitt uppdrag på ett effektivt och framgångsrikt sätt (Säkerhetspolisens hemställan Säkerhetspolisens informationshantering, Ju2022/02624). Sammantaget finns det starka skäl för en översyn av den reglering som styr Säkerhetspolisens behandling av personuppgifter.

Närmare om dagens regelverk och de begränsningar det medför

Regleringen av Säkerhetspolisens personuppgiftshantering fanns tidigare i den numera upphävda polisdatalagen (2010:361). Många av bestämmelserna togs i princip oförändrade in i Säkerhetspolisens datalag och har därför inte fullt ut anpassats till de behov som Säkerhetspolisen har i dag. Dagens regelverk och några av de begränsningar det medför beskrivs nedan.

Rättslig grund och ändamålsbestämmelser

Av 2 kap. 1 § Säkerhetspolisens datalag framgår att personuppgifter får behandlas om det är nödvändigt för att Säkerhetspolisen ska kunna utföra vissa i paragrafen uppräknade uppgifter. Uppgifterna korresponderar i princip med 3 § polislagen (1984:387) som anger Säkerhetspolisens huvudsakliga uppgifter, bl.a. att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet och terrorbrott samt för att utreda eller lagföra sådana brott. Nödvändighetsrekvisitet innebär i detta sammanhang att personuppgiftsbehandlingen ska behövas för att uppgiften ska gå att fullgöra på ett effektivt sätt (prop. 2018/19:163 s. 65 och 217). När det gäller känsliga personuppgifter krävs dessutom att behandlingen är absolut nödvändig i förhållande till ändamålet (2 kap. 9 § Säkerhetspolisens datalag).

Säkerhetspolisen får bara behandla personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål (2 kap. 3 § Säkerhetspolisens datalag). Att ändamålen ska vara särskilda innebär att de måste vara tillräckligt specificerade för att ge ledning för bedömningen av vilka uppgifter som är adekvata och relevanta för den aktuella behandlingen och för att det ska kunna avgöras att inte för många uppgifter behandlas. Att ändamålen ska vara berättigade innebär en koppling till den rättsliga grunden. Personuppgifter får således inte behandlas för ett ändamål som inte är berättigat i förhållande till den tillämpliga rättsliga grunden.

I Säkerhetspolisens underrättelseverksamhet, där personuppgifter behöver behandlas på ett tidigt stadium i processen, är det långt ifrån alltid möjligt att ange ändamålen med behandlingen lika tydligt och detaljerat som i annan brottsbekämpande verksamhet. I förarbetena till Säkerhetspolisens datalag framfördes mot den bakgrunden att det får accepteras att beskrivningen av ändamålen inte alltid kan ha samma precision som i annan brottsbekämpande verksamhet. Det finns vidare inget som hindrar att det närmare ändamålet med behandlingen inledningsvis är detsamma som det

som anges i bestämmelsen om rättslig grund. Ändamålet får sedan preciseras mer när det är möjligt (prop. 2018/19:163 s. 68).

Trots att Säkerhetspolisens datalag alltså är avsedd att ge generösare ramar för personuppgiftsbehandlingen än brottsdatalagen kan regleringen försvåra en effektiv informationshantering. Bestämmelserna om rättslig grund och ändamål innebär i praktiken att Säkerhetspolisen inte i alla situationer kan inhämta och på annat sätt behandla uppgifter som kan vara avgörande för att till exempel identifiera en okänd terrorist, spion eller annan antagonist eller för att hindra ett attentat. Skälet är att vissa uppgiftssamlingar som Säkerhetspolisen skulle vilja inhämta till stor del innehåller uppgifter om enskilda som inte har eller kan antas ha en klar koppling till Säkerhetspolisens brottsbekämpande verksamhet, men där en delmängd av informationen kan vara avgörande. För att kunna hitta den värdefulla informationen skulle myndigheten behöva inhämta och behandla personuppgifter från hela uppgiftssamlingen, även om det på förhand står klart att majoriteten av uppgifterna inte uppfyller kravet på nödvändighet om man ser på varje uppgift för sig. Om det till exempel kan förmodas att ett attentat planeras eller kan komma att planeras i en viss miljö, digital eller fysisk, kan Säkerhetspolisen behöva inhämta och bearbeta information från hela miljön. Det kan handla om att inhämta informationsmängder från öppna källor, till exempel sådan information som är tillgänglig för var och en via internet. För att kunna utnyttja den information som finns tillgänglig på ett effektivt sätt skulle Säkerhetspolisen behöva rättsliga förutsättningar för att till exempel samla in och göra jämförelser av fenomen och begrepp som förekommer i sociala medier med hjälp av automatiska processer.

Granskning av uppgifter och kravet på särskilda upplysningar

Om det behövs för att utföra någon av de uppgifter som anges i 2 kap. 1 § Säkerhetspolisens datalag, får personuppgifter göras gemensamt tillgängliga i Säkerhetspolisens verksamhet (3 kap. 2 §). För gemensamt tillgängliga uppgifter ska det genom en särskild upplysning anges för vilket ändamål uppgifterna behandlas om det inte framgår av sammanhanget eller på något annat sätt (3 kap. 3 §). Att en sådan upplysning om ändamålet ska anges har motiverats både av hänsyn till verksamheten och till den personliga integriteten. En upplysning om ändamålet kan också vara en förutsättning för att tillsynsmyndigheten ska kunna kontrollera att viss behandling är berättigad och görs i enlighet med lagens bestämmelser (prop. 2018/19:163 s. 88).

Att tillföra upplysningar om ändamålet med behandlingen av uppgifterna är mycket resurskrävande när det handlar om stora informationsmängder. Samtidigt som sådana upplysningar behöver tillföras måste Säkerhetspolisen också granska om det förekommer känsliga personuppgifter i materialet. Det sker i dag genom att handläggare granskar materialet manuellt. I många fall är det inte möjligt att genomföra en sådan kontroll när det handlar om större informationsmängder. Det kan exempelvis handla om hela trådar i ett forum eller aktiviteter kopplade till en viss person. Det leder i sin tur till att den här typen av inhämtning inte utförs, trots att det skulle kunna vara av stor vikt för Säkerhetspolisens arbete.

Behandling i syfte att utveckla datasystem m.m.

För att på bästa sätt kunna utnyttja de tekniska möjligheter som numera finns att behandla stora informationsmängder automatiskt måste programvarans förmåga utvecklas. För att kunna utveckla programvarans förmåga på ett ändamålsenligt sätt krävs behandling av stora datamängder av olika uppgiftsslag. Med nuvarande regelverks krav på att behandlingen av personuppgifter ska vara nödvändig i förhållande till den rättsliga grunden är det osäkert om behandling av personuppgifter över huvud taget kan ske i syfte att utveckla datasystem och träna upp modeller för maskininlärning. Enligt Säkerhetspolisen är det viktigt att myndigheten får möjlighet att behandla stora mängder relevanta data i syfte att utveckla tekniska lösningar så att de fungerar på bästa sätt.

Längsta tid för behandling

I 4 kap. Säkerhetspolisens datalag finns bestämmelser om hur länge personuppgifter får behandlas. Syftet med bestämmelserna är att skydda den personliga integriteten. Allmänt gäller att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (4 kap. 1 §). Därutöver finns särskilda regler för olika situationer. Personuppgifter som inte har gjorts gemensamt tillgängliga får till exempel inte behandlas längre än ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende. Personuppgifter som gjorts gemensamt tillgängliga får inte behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

På grund av den långsiktighet som präglar framför allt kontraspionage-verksamheten förlängdes tiden som den typen av uppgifter får behandlas när Säkerhetspolisens datalag infördes. Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt, får behandlas högst 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet. Säkerhetspolisen ansåg i samband med lagstiftningsärendet att sådana personuppgifter borde få behandlas som längst i 70 år. Säkerhetspolisen har nu framfört synpunkter på att bestämmelserna i kapitlet medför att uppgifter som i ett senare skede skulle kunna vara avgörande i t.ex. arbetet med kontraspionage eller kontraterrorism inte får behandlas tillräckligt länge. Säkerhetspolisen behöver kunna behandla uppgifterna över tid för att bearbeta informationen och därmed kunna upptäcka mönster eller samband.

Uppdraget att se över Säkerhetspolisens personuppgiftsreglering i syfte att skapa ändamålsenliga regler som är anpassade efter dagens behov

Säkerhetspolisen har pekat på att regelverket som styr myndighetens personuppgiftshantering inte alltid ger förutsättningar för att samla in och behandla uppgifter som kan vara avgörande i verksamheten. Det är mycket angeläget att Säkerhetspolisen har ändamålsenliga bestämmelser i detta avseende. Den nuvarande lagstiftningen fungerar i vissa avseenden väl. Samtidigt stöter Säkerhetspolisen i dag på problem bland annat vid tillämpningen av de i Säkerhetspolisens datalag fundamentala bestämmelserna om rättslig grund och ändamål för behandlingen. Utredarens övergripande uppdrag är därför att göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Syftet är att skapa ändamålsenliga regler som är anpassade efter dagens behov och möjligheter. De författningar som står i fokus är Säkerhetspolisens datalag med tillhörande förordning. Ovan har några av de begränsningar som Säkerhetspolisen lyft fram beskrivits. Uppdraget att göra en översyn av regleringen gäller emellertid inte endast dessa begränsningar.

Beträffande flera andra myndigheter finns förslag eller pågående lagstiftningsarbete som tar sikte på ökade möjligheter att använda dataanalyser och urval för att effektivisera informationshanteringen i verksamheten (se t.ex. dir. 2021:104, En modern dataskyddsreglering för

Skatteverket, Tullverket och Kronofogdemyndigheten och förbättrade förutsättningar för en effektiv kontrollverksamhet). Utifrån Säkerhetspolisens uppdrag som nationell säkerhetstjänst och med tanke på Säkerhetspolisens underrättelse- och säkerhetsarbete finns det goda skäl för att myndigheten bör ha ett mer generöst regelverk kring personuppgiftsbehandlingen än många andra myndigheter. I Norge pågår också lagstiftningsarbete för att ge ökade möjligheter för säkerhetstjänsten (Politiets sikkerhetstjeneste) att behandla stora informationsmängder med hjälp av tekniska hjälpmedel.

Mot den bakgrunden bör en utgångspunkt för översynen vara att Säkerhetspolisen ska få ökade möjligheter att behandla personuppgifter, t.ex. genom att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel. Detta är också utredningens huvudfokus. Reglerna behöver vara teknikneutrala och flexibla samt ge Säkerhetspolisen möjlighet att utveckla och anpassa arbetet efter samhällsutvecklingen.

Uppdraget omfattar endast Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet, och alltså inte den behandling som ligger inom brottsdatalagens tillämpningsområde. Det ligger heller inte inom ramen för utredarens uppdrag att se över sekretessregleringen som kan påverka vilka uppgifter Säkerhetspolisen har möjlighet att ta del av. Däremot kan det finns behov av sekretessregler för att skydda den informationshantering som utredarens förslag kan medföra.

Utredaren ska

- göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet,
- beskriva dagens rättsliga möjligheter för Säkerhetspolisen att behandla personuppgifter, särskilt vad gäller att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel,
- undersöka i vilken utsträckning dagens regelverk försvårar en effektiv informationshantering i Säkerhetspolisens verksamhet,
- lämna förslag som gör att information kan hanteras av Säkerhetspolisen på ett mer ändamålsenligt sätt än i dag, och
- lämna nödvändiga författningsförslag.

Utredaren ska noga väga Säkerhetspolisens behov av att behandla personuppgifter mot den enskildes rätt till skydd för sin personliga integritet. Särskilda integritetsskyddande åtgärder bör därvid övervägas.

Utredaren ska också vid utformningen av förslagen beakta att tillsynsmyndigheterna ska ges förutsättningar att kunna fullgöra sin uppgift att utöva tillsyn över personuppgiftsbehandlingen på ett effektivt sätt. Om det bedöms nödvändigt får utredaren ta upp andra närliggande frågor i samband med de frågeställningar som ska utredas.

Grundläggande fri- och rättigheter ska beaktas

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Inskränkningar i det grundlagsfästa skyddet kan endast göras genom lag och bara under de förutsättningar som anges i 2 kap. 20–22 och 25 §§ regeringsformen.

Rätten till respekt för privat- och familjelivet och för korrespondens skyddas också av bl.a. artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och artikel 16 i FN:s konvention om barnets rättigheter (barnkonventionen). Vidare framgår det av artikel 3 i barnkonventionen att vid samtliga åtgärder och beslut som rör barn ska i första hand vad som bedöms vara barnets bästa beaktas.

Detta grundläggande skydd för enskildas integritet är inte absolut. Av såväl regeringsformen som Europakonventionen framgår att skyddet under vissa förutsättningar får begränsas. En begränsning i utövande av rättigheten får göras endast om det sker i enlighet med lag och det är nödvändigt för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den.

Att föreslå grundlagsändringar ingår inte i utredarens uppdrag. De förslag som utredaren lämnar måste alltså vara förenliga med regeringsformen och naturligtvis också med Europakonventionen, barnkonventionen och Sveriges internationella förpliktelser i övrigt.

Dataskyddskonventionen måste beaktas

Eftersom varken dataskyddsdirektivet eller dataskyddsförordningen omfattar behandling av personuppgifter som utförs i verksamhet som rör nationell säkerhet finns det ur EU-rättslig synvinkel inte något som hindrar att regleringen som styr Säkerhetspolisens personuppgiftsbehandling i den delen utformas på ett annat sätt än det EU-rättsliga regelverket. Europarådets ministerkommitté antog 1981 en konvention till skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen. Konventionen var en av de viktigaste inspirationskällorna vid utformningen av EU:s regelverk för dataskydd. Konventionen gäller även i verksamhet som rör nationell säkerhet och Sverige är folkrättsligt bundet av konventionen med dess tilläggsprotokoll. En särreglering av Säkerhetspolisens personuppgiftsbehandling får alltså inte strida mot bestämmelserna i dataskyddskonventionen (se t.ex. prop. 2018/19:163 s. 50).

Eftersom det EU-rättsliga regelverket bygger på och vidareutvecklar dataskyddskonventionen liknar många bestämmelser varandra. I dataskyddskonventionen finns det exempelvis bestämmelser om att personuppgifter ska behandlas på ett korrekt och lagligt sätt och att de ska lagras för särskilt angivna och lagliga ändamål och inte användas på ett sätt som är oförenligt med dessa ändamål samt att de ska bevaras på ett sådant sätt att de registrerade personerna inte kan identifieras under längre tid än vad som är nödvändigt med hänsyn till det ändamål för vilket dessa uppgifter lagras (artikel 5). Till skillnad från i det EU-rättsliga regelverket finns dock möjligheter att göra undantag från de grundläggande bestämmelserna. Undantag får göras endast om en sådan avvikelse medges i nationell lagstiftning och den är nödvändig i ett demokratiskt samhälle för att skydda statens säkerhet, den allmänna säkerheten, statens penningintressen eller brottsbekämpning samt för att skydda den registrerade personen eller andra personers fri- och rättigheter (artikel 9).

Konventionen kompletteras av ett antal av ministerkommittén antagna rekommendationer om hur personuppgifter bör behandlas inom olika områden. En sådan rekommendation rör behandling av stora datamängder (Council of Europe, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 17 January 2017). I syfte att modernisera konventionen har en översyn av den pågått inom Europarådet. Förhandlingarna resulterade i maj 2018 i att ett

ändringsprotokoll antogs. Ändringsprotokollet innebär bland annat att möjligheterna att göra undantag från de grundläggande principerna om dataskydd blir mindre än i nuvarande utformning. Sverige tillhörde de första konventionsstaterna att underteckna protokollet. Ändringsprotokollet träder dock inte i kraft förrän alla parter har ratificerat protokollet (eller om minst 38 parter har gjort det den 11 oktober 2023).

Utredarens förslag måste anpassas till bestämmelserna i dataskyddskonventionen med ändringsprotokoll.

Konsekvensbeskrivningar

Utredaren ska utöver vad som följer av kommittéförordningen (1998:1474) noga analysera vilka konsekvenser de förslag som lämnas har för den personliga integriteten. Utredaren ska också bedöma hur förslagen förhåller sig till Sveriges internationella åtaganden om mänskliga rättigheter.

Kontakter och redovisning av uppdraget

Utredaren ska under arbetet samråda med och hämta in synpunkter och upplysningar från Säkerhetspolisen. Vid behov ska utredaren hämta in synpunkter och upplysningar även från andra myndigheter och aktörer som kan vara berörda. Utredaren ska också följa utvecklingen beträffande de rättsliga förutsättningarna för säkerhetstjänstens informationshantering i Norge, och vid behov även i andra länder. Utredaren ska också hålla sig informerad om och ta hänsyn till relevant arbete som pågår inom Regeringskansliet och kommittéväsendet samt inom ramen för Sveriges internationella åtaganden.

Uppdraget ska redovisas senast den 15 november 2024.

(Justitiedepartementet)