Dataskyddspolicy

210914

POLICY

Fastställd av GD: 14 september 2021
Träder i kraft: 14 september 2021
Upphör att gälla: 14 september 2024

Ansvarig: ML/S/RS
Dnr: A2021/2963
Version: 1.0

Dataskyddspolicy

Statistiska centralbyråns dataskyddspolicy slår fast myndighetens tolkning av rättsliga grunder för behandling av personuppgifter på myndigheten enligt dataskyddsförordningen.

Inledning

Dataskyddsförordningen[1] tillämpas sedan den 25 maj 2018 i hela EU och övriga länder i EES. Den är direkt tillämplig på all behandling av personuppgifter i EU och därför på Statistiska centralbyrån (SCB). För att SCB ska kunna uppfylla vissa certifieringskrav, behöver myndighetens tolkning bland annat av de rättsliga grunderna för behandling av personuppgifter enligt dataskyddsförordningen slås fast i en policy.

Tillämpning av dataskyddsförordningen

Dataskyddsförordningen gäller för 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. Den gäller i princip inom all slags verksamhet och oavsett vem som utför personuppgiftsbehandlingen, för myndigheter och för privata företag och organisationer.

En fysisk person som behandlar personuppgifter som ett led i verksamhet av rent privat natur eller som har samband med personens hushåll är undantagen från förordningens tillämpning. Undantag gäller även för yttranden inom ramen för yttrandefriheten och för utlämnande av handlingar enligt offentlighetsprincipen.

Dataskyddsförordningen ska tillämpas på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i EU, oavsett om behandlingen utförs i EU eller inte.

För SCB innebär detta att hela myndighetens behandling av personuppgifter styrs av dataskyddsförordningen, även i verksamhet inom ramen för internationella samarbeten utanför EU. SCB:s publicering av tidskrifter, publicering på internet samt utlämnande av handlingar enligt offentlighetsprincipen sker dock enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen, då gäller inte dataskyddsförordningen.

Regler om detta finns i art. 2, 3, 85 och 86 dataskyddsförordningen samt 2 kap. 7 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Personuppgift

Med personuppgift menas varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person. Typiska personuppgifter är personnummer, namn och adress. Bilder på, och ljudupptagningar av, personer kan vara personuppgifter om personerna kan identifieras. Även information som har kodats, krypterats eller pseudonymiserats men som kan hänföras till en fysisk person

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

med hjälp av kompletterande uppgifter är personuppgifter. Elektroniska uppgifter som IP-adresser och kakor kan också vara personuppgifter.

SCB använder ofta personuppgifter i sin verksamhet för att framställa statistik. Personuppgifter förekommer också i så gott som all annan verksamhet som SCB bedriver vid sidan om den statistiska verksamheten.

Termen personuppgift definieras i art. 4.1 dataskyddsförordningen.

Känsliga personuppgifter

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd i dataskyddsförordningen. De brukar kallas känsliga personuppgifter. Utgångspunkten är att behandlingen av sådana uppgifter är förbjuden, om det inte finns särskilda bestämmelser som tillåter behandlingen.

Känsliga personuppgifter är sådana uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Därtill kommer personuppgifter som rör lagöverträdelse som innefattar brott.

Känsliga personuppgifter används i vissa fall för att framställa statistik på SCB. De förekommer också i personaladministration och kan förekomma i annan verksamhet.

Regler om detta finns i art. 9 och 10 dataskyddsförordningen.

Principer för behandling av personuppgifter

I dataskyddsförordningen finns vissa grundläggande principer som ska uppfyllas vid all behandling av personuppgifter och under hela den tid som en behandling pågår. Det finns följande principer:

- *Laglighet, korrekthet och öppenhet* innebär bland annat att det måste finnas en rättslig grund för behandlingen, att behandlingen ska vara rimlig och proportionerlig i förhållande till de registrerade och att det ska vara klart och tydligt för de registrerade hur deras personuppgifter behandlas.

- *Ändamålsbegränsning* innebär att personuppgifter bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att de inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål är tillåtna. – Regeln om statistiska ändamål är ofta tillämplig i SCB:s verksamhet och för uppgiftslämnare till SCB:s statistik.

- *Uppgiftsminimering* innebär att personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålen.

- *Riktighet* innebär att personuppgifterna ska vara riktiga och uppdaterade.

- *Lagringsminimering* innebär att personuppgifter inte får sparas i identifierbart skick under en längre tid än vad som är nödvändigt för ändamålen med behandlingen.

- *Integritet och konfidentialitet* innebär att den som behandlar personuppgifter ska vidta lämpliga åtgärder för att skydda uppgifterna så att de inte blir åtkomliga för obehöriga, förstörs eller skadas.

- *Ansvarsskyldighet* innebär att den som behandlar personuppgifter ansvarar för att de grundläggande principerna uppfylls och ska kunna visa på vilket sätt principerna uppfylls.

Varje person som arbetar på eller för SCB i verksamhet som rör personuppgifter ska känna till att det finns fastslagna principer för behandlingen av personuppgifter. På SCB innebär lagringsminimering bland annat att temporära filer ska tas bort.

Regler om detta finns i art. 5 dataskyddsförordningen.

Rättslig grund för behandling av personuppgifter

För att en behandling av personuppgifter ska vara tillåten krävs att det finns en rättslig grund för behandlingen. Följande rättsliga grunder för behandling finns:

a. den registrerade personen 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.

Den rättsliga grunden enligt f gäller inte för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

För SCB som myndighet gäller att den övervägande delen av all personuppgiftsbehandling har rättslig grund enligt e. Uppgifter av allmänt intresse måste vara fastställt i EU-rätten eller nationell rätt, och är för SCB:s räkning fastställd i lagen (2001:99) om den officiella statistiken, förordningen (2001:100) om den officiella statistiken, förordningen (2016:822) med instruktion för Statistiska centralbyrån och olika specialbestämmelser.

Det förekommer också personuppgiftsbehandling hos SCB grundat på b, c eller d. Ytterst sällan behandlas personuppgifter på en myndighet enligt a, och detta bör undvikas genom att först fastställa att någon annan rättslig grund är tillämplig. Flera rättsliga grunder kan föreligga samtidigt, men det måste alltid finnas minst en rättslig grund att tillämpa.

Vid all produktion av statistik måste behandlingen av personuppgifter ha sin rättsliga grund enligt någon av de ovanstående punkterna. Det finns särskilda undantag för bland annat statistik, när det gäller de ändamål för vilka data samlas in, se föregående avsnitt. Dessa undantag påverkar inte behovet av att ha en rättslig grund för behandlingen av personuppgifterna.

Regler om detta finns i art. 6 dataskyddsförordningen.

Personnummer

Medlemsstaterna får närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Ett sådant identifikationsnummer ska då endast användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt dataskyddsförordningen.

För svensk del räknas personnummer som nationellt identifikationsnummer. Personnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. En statistikansvarig myndighet får behandla personnummer för framställning av statistik.

SCB använder som regel personnummer vid framställning av statistik. Även samordningsnummer och andra, tillfälliga identiteter förekommer. Det är klart motiverat av flera skäl. Personnummer används bland annat för att kunna följa personer i tidsserier och för att lätt kunna åldersbestämma personer och dela upp statistiken efter kön. SCB:s rutiner för att ta fram registerutdrag enligt art. 15 dataskyddsförordningen bygger på sökning på personnummer.

Regler om detta finns i art. 87 dataskyddsförordningen, 3 kap. 10 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning och 14 § andra stycket lagen om den officiella statistiken.

Inbyggt dataskydd och dataskydd som standard

En personuppgiftsansvarig ska genomföra lämpliga tekniska och organisatoriska åtgärder så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas. Det gäller både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen. Pseudonymisering av personuppgifter är en sådan åtgärd. Åtgärderna ska utformas för att principer för dataskydd ska kunna genomföras effektivt, exempelvis genom uppgiftsminimering. De nödvändiga skyddsåtgärderna ska integreras i behandlingen. Dessa åtgärder ska ske 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.

Den personuppgiftsansvarige ska 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.

SCB behandlar många personuppgifter elektroniskt. Det är därför viktigt att IT-systemen utformas på ett sätt som redan från början har tillräckliga inbyggda dataskydd. Det ska finnas dataskydd som standard i allt utvecklingsarbete. SCB:s organisation ska också vara utformad för att begränsa tillgången till personuppgifter genom aktiv och aktuell behörighetsstyrning. Personer som inte behöver ha tillgång till vissa personuppgifter för att utföra sina arbetsuppgifter ska inte ha det. SCB genomför löpande och årliga revisioner av behörighetsstyrningen.

Regler om detta finns i art. 25 dataskyddsförordningen.

Personuppgiftsansvarig och personuppgiftsbiträde

SCB är normalt personuppgiftsansvarig för den behandling av personuppgifter som utförs på myndigheten. Det förekommer även att SCB är personuppgiftsbiträde. Så kan vara fallet när SCB framställer statistik åt andra statistikansvariga myndigheter och så är fallet när SCB lämnar ut större mängder data till externa mottagare som får del av detta på en databas som SCB driftar. När SCB anlitar personuppgiftsbiträde eller är personuppgiftsbiträde åt annan, tecknas alltid personuppgiftsbiträdesavtal. I SCB:s mall för personuppgiftsbiträdesavtal finns en bilaga där tekniska krav på biträdet specificeras.

Regler om detta finns i art. 4.7, 4.8, 24 och 28 dataskyddsförordningen och 14 § första och tredje styckena lagen om den officiella statistiken.

Överföring av personuppgifter till tredjeland

Överföring av personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation får bara ske under särskilda förutsättningar. Med tredjeland avses varje land utanför EU och EES.

EU-kommissionen kan besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. I övrigt finns detaljerade regler för att säkerställa att överföring av personuppgifter är säkert samt undantagsregler för särskilda fall.

SCB överför som regel bara personuppgifter till mottagare i tredjeland när det finns ett beslut av EU-kommissionen om adekvat skyddsnivå för det landet, eller enligt undantagsregler för särskilda fall.

Regler om detta finns i art. 44–50 dataskyddsförordningen.

Organisation

En förvaltningsmyndighet som behandlar personuppgifter ska utse ett dataskyddsombud. Även andra personuppgiftsansvariga och personuppgiftsbiträden ska under vissa förutsättningar utse ett dataskyddsombud. Det gäller till exempel om de har en kärnverksamhet som består av behandling i stor omfattning av känsliga personuppgifter. Dataskyddsombudet ska ha en självständig ställning och vara bundet av sekretessregler. Med hänsyn till organisationsstruktur och storlek kan ett dataskyddsombud utses för flera myndigheter.

SCB har, som stor myndighet med omfattande behandling av personuppgifter, utsett ett eget dataskyddsombud.

Regler om detta finns i art. 37 och 38 dataskyddsförordningen.

Dataskyddsombudet ska informera och ge råd till den personuppgiftsansvarige och de anställda som behandlar personuppgifter, om deras skyldigheter enligt dataskyddsförordningen och andra av unionens eller medlemsstaternas dataskyddsbestämmelser. Vidare ska dataskyddsombudet övervaka efterlevnaden av dataskyddsförordningen och andra regelverk i EU, Sverige och hos den personuppgiftsansvarige, på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den, samarbeta med Integritetsskyddsmyndigheten som svensk tillsynsmyndighet, samt att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling av personuppgifter och vid behov samråda i alla andra frågor.

SCB:s dataskyddsombud rapporterar direkt till generaldirektören, men ger stöd åt hela myndigheten. Det går att nå dataskyddsombudet på mail på dataskyddsombud@scb.se.

Regler om detta finns i art. 39 dataskyddsförordningen.