



## DATASKYDDSPOLICY

### Inledning

Dataskyddsförordningen<sup>1</sup> började tillämpas den 25 maj 2018 i hela EU. Den är därför direkt tillämplig på all behandling av personuppgifter 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 unionen, oavsett om behandlingen utförs i unionen 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 och på internet samt utlämnande av handlingar enligt offentlighetsprincipen sker enligt samma regler som alltid.

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.

---

<sup>1</sup> 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).



## Vad som menas med 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 med hjälp av kompletterande uppgifter är 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.

Personuppgift definieras i art. 4.1 dataskyddsförordningen.

## Vad som menas med känslig personuppgift

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 många fall för att framställa statistik på SCB. Det förekommer också i exempelvis personaladministration och liknande. Det finns ingen verksamhet där det helt kan utslutas att känsliga personuppgifter kan förekomma. Det är därför viktigt för alla medarbetare att tänka på om känsliga personuppgifter förekommer i verksamheten.

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.

- *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. För SCB:s räkning är det viktigt att känna till att data som har samlats in för ett visst ändamål även får användas för vissa andra ändamål, exempelvis statistiska ändamål.

Regler om detta finns i art. 5 dataskyddsförordningen.

## **Rättslig grund för behandling av personuppgifter**

Behandling av alla personuppgifter är tillåten – om det inte gäller känsliga personuppgifter enligt ovan – så länge 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 (2016:822) med instruktion för SCB 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 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.

### **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 till personer som inte behöver ha tillgång till uppgifterna för att utföra sina arbetsuppgifter.

Regler om detta finns i art. 25 dataskyddsförordningen.

## Organisation

En myndighet som behandlar personuppgifter ska utse ett dataskyddsombud. Skyldigheten att utse ett dataskyddsombud gäller dock inte när behandlingen sker som en del av domstolars dömande verksamhet. 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 denna förordning 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 Datatinspektionen 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 har ett dataskyddsombud på heltid. Dataskyddsombudet rapporterar direkt till generaldirektören, men är tillgängligt för hela myndigheten. Det går att nå dataskyddsombudet på mail internt på \*Dataskyddsombud eller externt på [dataskyddsombud@scb.se](mailto:dataskyddsombud@scb.se).

Regler om detta finns i art. 39 dataskyddsförordningen.