RIKTLINJER FÖR BEHANDLING AV PERSONUPPGIFTER ENLIGT DATASKYDDSFÖRORDNINGEN

INLEDNING

Dataskyddsförordningen, GDPR, (förkortning av engelskans General Data Protection Regulation) och datalagen, båda kallas i det följande gemensamt för dataskyddsförordningen, innehåller bl a bestämmelser om när personuppgifter får samlas in, hur de insamlade personuppgifterna får behandlas, informationsskyldighet, anmälan av personuppgiftsincidenter, rätten att bli bortglömd samt möjlighet att utdöma ekonomiska sanktioner mot personuppgiftsansvarig som bryter mot dataskyddsbestämmelsernas regler.

ALLMÄNNA BESTÄMMELSER

Förhållande till offentlighet, tryck- och yttrandefrihet

Bestämmelserna i dataskyddsförordningen är inte tillämpliga om de strider mot bestämmelserna i tryckfrihetsförordningen, yttrandefrihetsgrundlagen eller offentlighetsprincipen. Exempelvis tillämpas i princip inte dataskyddsförordningen om någon begär att få ut allmän handling.

Personuppgiftsansvarig

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer varför och hur behandling av personuppgifter ska ske. I kommunen är varje nämnd personuppgiftsansvarig inom sitt verksamhetsområde. Det fulla ansvaret för behandling av personuppgifter vilar på den personuppgiftsansvarige, även när det finns ett dataskyddsombud och/eller ett personuppgiftsbiträde.

Personuppgiftsbiträde

Personuppgiftsbiträdet är den som anlitas av den personuppgiftsansvarige för behandling av personuppgifter. Biträdet är alltid någon utanför nämnden och är aldrig någon som är anställd av nämnden. Ett personuppgiftsbiträde kan vare en fysisk eller en juridisk person. Den personuppgiftsansvarige ansvarar för att det finns skriftligt avtal med personuppgiftsbiträdet som bara får behandla uppgifter i enlighet med den ansvariges instruktioner.

Dataskyddsombud

Dataskyddsombudet ska informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar personuppgifter om deras skyldigheter enligt dataskyddsförordningen och övriga dataskyddsbestämmelser. Vidare ska dataskyddsombudet övervaka efterlevnaden av dataskyddsförordningen och övriga dataskyddsbestämmelser. Dessutom ska dataskyddsombudet på begäran ge råd vad gäller konsekvensbedömning avseende dataskydd och övervaka genomförandet av denna.

Dataskyddsombudet ska samarbeta med tillsynsmyndigheten samt fungera som kontaktpunkt för tillsynsmyndigheten.

Kontaktperson

Den fysiska person inom nämnden som ansvarar för att utföra det arbete som ligger inom den personuppgiftsansvariges ansvarsområde samt ha kontakt med dataskyddsombudet.

Vad är en personuppgift?

En personuppgift är varje upplysning som avser en identifierad eller identifierbar fysisk person.

En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras, till exempel med ett namn, personnummer eller samordningsnummer (identitetsbeteckning för personer som inte är eller har varit folkbokförda i Sverige), en lokaliseringsuppgift eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, biometriska, psykiska, ekonomiska, kulturella eller sociala identitet.

Även s k ostrukturerad behandling av personuppgifter, dvs behandling av personuppgifter i löpande text i ordbehandlingsprogram, löpande text på internet, ljud- och bildupptagningar och e-post omfattas av dataskyddsförordningen. Varje medarbetare ansvarar för att personuppgifter som denne hanterar ostrukturerat behandlas på ett relevant och riktigt sätt samt att aktuell behandling av dessa personuppgifter är tillåten.

Begreppet personuppgift är brett och innefattar både text, bild och ljud.

Dataskyddsförordningen gäller enbart behandling av personuppgifter knutna till levande personer.

Uppgifter om juridiska personer omfattas inte av definitionen även om den juridiska personen råka ägas av en eller ett fåtal fysiska personer eller ha en benämning som innefattar ett personnamn. Däremot omfattas enskild firma eftersom innehavaren av en sådan firma alltid är en fysisk person.

Behandling av personuppgifter

Behandling är en åtgärd eller kombination av åtgärder beträffande personuppgifter oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, radering eller förstöring.

Lagliga grunder för behandling

Dataskyddsförordningen anger att varje behandling av personuppgifter måste vila på en laglig grund. Behandling får därför bara ske under de omständigheter som särskilt anges i lagstiftningen. Någon av följande lagliga grunder eller kombination av grunder måste vara för handen för att en organisation ska få behandla varje enskild personuppgift:

1 Samtycke

2 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
3 Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige
4 Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person
5 Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
6 Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre eller kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

GRUNDLÄGGANDE KRAV PÅ BEHANDLING AV PERSONUPPGIFTER

Dataskyddsförordningen ställer grundläggande krav på att all behandling måste vara laglig, i betydelsen att någon av de lagliga grunder som anges i dataskyddsförordningen är uppfylld. Dessutom omgärdas varje behandling av personuppgifter av mer specifika krav.

Den första principen är att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Vidare ska personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får inte behandlas på ett sätt som är oförenligt med dessa ändamål. Ett ändamål som inte är berättigat i förhållande till den tillämpliga lagliga grunden är alltså inte förenligt med dataskyddsförordningen.

Myndigheten som behandlar personuppgifter måste leva upp till principerna för behandling av personuppgifter och laglig behandling av dessa i dataskyddsförordningen. Detta innebär att följande sju principer gäller för all behandling:

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

Samtycke

Allmänt för samtycke gäller att detta ska vara frivilligt, specifikt och informerat på sådant sätt att det otvetydigt framgår att den registrerade godkänner behandlingen av sina personuppgifter. Underförstådda samtycken är inte acceptabla (ex tystnad, på förhand

ikryssade rutor). Den registrerade har rätt att återkalla sitt samtycke. Respektive myndighet ska ha utformade samtyckestexter.

Behandling av personuppgifter vid erbjudande av informationssamhällets tjänster direkt till ett barn är tillåten med stöd av barnets samtycke om barnet är minst 13 år, i annat fall är den tillåten endast om samtycke ges av den som har föräldraansvaret.

Behandling av känsliga personuppgifter

Vissa personuppgifter är känsliga personuppgifter. Det är uppgifter som rör ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om fysisk persons sexualliv eller sexuella läggning.

Känsliga personuppgifter får behandlas om den registrerade lämnar ett uttryckligt samtycke, vilket är högre krav en ”vanliga” samtycken.

Ytterligare undantag finns om behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter när viktigt allmänt intresse föreligger samt inom bl a arbetsrätten, hälso- och sjukvården, social omsorg, arkivverksamhet och för statistiska ändamål.

Personnummer och samordningsnummer

Personnummer eller samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av säker identifiering eller något annat beaktansvärt skäl.

Pseudonymiserade uppgifter, skyddade personuppgifter

Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Hos Skatteverket finns skyddade personuppgifter som sekretessmarkering, kvarskrivning och fingerade personuppgifter).

Arkivering och gallring

Att spara handlingar som innehåller personuppgifter är en sorts behandling. Personuppgifter får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. När personuppgifterna inte längre behövs måste de gallras. Det är alltså ändamålet med inhämtningen av personuppgifter som avgör hur länge personuppgifter får bevaras. Personuppgifter får dock bevaras i enlighet med arkivlagen, arkivförordningen och kommunens arkivreglemente.

Dokumentation

Varje myndighet ska föra register för varje behandling av personuppgifter i verksamheten. Registerförteckningen ska minst innehålla följande uppgifter:

1. Namn och kontaktuppgifter för den personuppgiftsansvarige, den personuppgiftsansvariges företrädare samt dataskyddsombud
2. Ändamålet med behandlingen
3. Kategorier av registrerade
4. Kategorier av personuppgifter
5. Kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut
6. Dokumentation om uppgifter överförs till tredje land (land utanför EU och EES)
7. Förutsedda tidsfrister för radering av de olika kategorierna av uppgifter
8. Allmän beskrivning av tekniska och organisatoriska skyddsåtgärder

I samband med inventeringen ska också säkerställas att personuppgiftsbehandlingarna är lagliga samt följer de grundläggande kraven på behandling.

För behandling av personuppgifter som innebär hög risk för fysiska personers rättigheter och friheter ska konsekvensbedömning genomföras i samarbete med dataskyddsombudet.

Se mall.

Informationsskyldighet

Dataskyddsförordningen innehåller krav på vilken information som ska lämnas till den registrerade. Uppgifterna kan komma från den registrerade eller från annan än den registrerade. Undantag kan finnas i speciallagstiftning.

Kommunen ger en generell information på kommunens hemsida.

Den registrerades rätt till tillgång till personuppgifter gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckningar eller liknande. Undantaget gäller inte om uppgifterna lämnats utanför myndigheten, behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål eller har behandlats under längre tid än ett år i löpande text som inte fått sin slutliga utformning.

Information om personuppgifterna samlats in från den registrerade ska lämnas när personuppgifterna erhålls, se mall.

Information som inte har erhållits från den registrerade ska lämnas vid någon av följande tidpunkter; inom rimlig tid dock senast inom en månad, vid tidpunkt för första kommunikation med den registrerade, när personuppgifterna lämnas ut första gången, se mall.

Den registrerade har rätt att ta del av de personuppgifter som rör hen hos personuppgiftsansvarig, se mall. Begränsningar kan finnas i lag.

Rättelse

Den vars personuppgifter är registrerade har rätt att vända sig till myndigheten som behandlar personuppgifterna och få felaktiga uppgifter rättade så fort som möjligt. Den enskilde har också rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med behandlingen. När myndigheten rättar uppgifter ska den registrerade meddelas att rättelse gjorts.

Radering

Dataskyddsförordningen ger vissa möjligheter för den registrerade att få personuppgifter raderade. Lagring av personuppgifter kan trots begäran om radering vara laglig om personuppgifterna krävs för att utöva yttrande- och informationsfrihet, för att uppfylla en rättslig förpliktelse, utföra uppgifter av allmänt intresse eller som ett led i myndighetsutövning, eller för fastställande, utövande eller försvar av rättsliga intressen.

Observera att den personuppgiftsansvarige aktivt ska radera uppgifter när dessa inte längre är aktuella för behandling.

Dataportabilitet

Den registrerade har rätt att få ut de personuppgifter som rör hen och som hen har tillhandahållit den personuppgiftsansvarige och har rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig om behandlingen grundas på ett samtycke och är automatiserad**.**

Ostrukturerade personuppgifter

I dataskyddsförordningen finns inte den så kallade missbruksregeln som tidigare kunde tillämpas för ostrukturerade personuppgifter (ex. löpande text, e-post och webbplatser) utan någon av dataskyddsförordningens lagliga grunder krävs för behandling.

Säkerhet

Användare ska inte ha större behörighet till personuppgifter än vad som är nödvändigt för att utföra arbetsuppgifter. Behörigheter som ska tilldelas beslutas av närmsta chef eller annan som är utsedd för uppgiften. För mobila enheter ska extra försiktighet iakttas.

Den som behandlar personuppgifter ska se till att ha en lämplig säkerhetsnivå för uppgifterna, både tekniskt och organisatoriskt. Vad som är en lämplig säkerhetsnivå beror på bland annat riskerna med behandlingen, vilken typ av uppgifter som behandlas, på de tekniska möjligheter som finns och på kostnaderna.

Vid riskbedömningen ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet risken för oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Pseudonymisering och kryptering av personuppgifter är exempel på åtgärder som minskar risken med behandlingen.

Personuppgiftsincidenter

Personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Det kan också vara fråga om en personuppgiftsincident om en säkerhetsincident leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna.

Anmälan om incidenter ska göras till Datainspektionen inom 72 timmar från det att man upptäckt vad som hänt. Syftet med anmälan är att göra det möjligt för Datainspektionen att se och bevaka vilka åtgärder som vidtas för att motverka negativa effekter av det inträffade. Den personuppgiftsansvarige, dvs nämnden, ska göra anmälan.

Datainspektionen har på sin hemsida e-tjänst för anmälan.

Den personuppgiftsansvarige är dessutom skyldig att, om det bedöms som sannolikt att hög risk för fysiska personers rättigheter och friheter föreligger, informera de personer vars uppgifter berörs av incidenten.

Dokumentation ska alltid ske av personuppgiftsincidenter, dvs vad som inträffat, dess effekter och vilka åtgärder som vidtagits.

Nämnden ska alltid kontakta kommunens Dataskyddsombud vid misstanke om personuppgiftsincidenter.

Sanktionsavgifter

I dataskyddsförordningen finns möjligheter för tillsynsmyndigheten att besluta om administrativa sanktionsavgifter. Detta gäller även statliga och kommunala myndigheter. För mindre allvarliga överträdelser uppgår avgiften för myndigheter till högst 5 miljoner kronor och för allvarligare överträdelser till högst 10 miljoner kronor. För andra organ är det maximala beloppet 20 miljoner euro eller 4 procent av ett företags globala omsättning. När tillsynsmyndigheten ska fastställa beloppet ska den ta hänsyn till en mängd omständigheter, som överträdelsens karaktär, svårighetsgrad och varaktighet, omfattning, syfte, antalet berörda registrerade och den skada de lidit. Även personuppgiftsbiträdet kan bli betalningsskyldig.

Tillsynsmyndighet

Datainspektionen är tillsynsmyndighet. Information om lagstiftningen och tillämpningen av denna finns på myndighetens hemsida. Vidare dömer Datainspektionen ut den administrativa sanktionsavgiften. Enskilda kan också vända sig till Datainspektionen med klagomål.

Lagstiftning mm

Länkar till dataskyddsförordningen, datalagen mm

Länk till DI och SKL