STRATEGI
PROGRAM
PLAN
POLICY
RIKTLINJER
REGLER

RIKTLINJER FÖR BEHANDLING AV PERSONUPPGIFTER I HÖGANÄS KOMMUNKONCERN

HÖGANÄS KOMMUN

Fastställt av: Kommunfullmäktige
Datum: 2022-04-28
För revidering ansvarar: Kommunkansliet
För eventuell uppföljning och tidplan ansvarar: Kommunkansliet
Dokumentet gäller för: Höganäs kommunkoncern
Dokumentet gäller till och med: Tillsvidare

RIKTLINJER FÖR BEHANDLING AV PERSONUPPGIFTER

Att värna den personliga integriteten för de personer vars personuppgifter behandlas i kommunkoncernens verksamheter är en viktig strategisk fråga för Höganäs kommunkoncern. I arbetet med personuppgiftsbehandling ska kommunkoncernen vara en bra part som arbetar förebyggande.

RIKTLINJERNAS OMFATTNING

Riktlinjer för behandling av personuppgifter är en konkretisering av Höganäs kommunkoncerns policy för informationssäkerhet och personuppgiftshantering KS/2019/255 och anger hur personuppgifter ska behandlas inom kommunkoncernen. Dessa riktlinjer gäller för alla verksamheter (samtliga nämnder och kommunala bolag inom Höganäs kommun) vilket innebär att det inte finns utrymme att besluta om lokala avvikelser. Alla medarbetare inom kommunkoncernen ska regelbundet informeras om och utbildas i innehållet i riktlinjerna enligt fastställd utbildningsplan. Bestämmelserna i riktlinjerna omfattar även externa parter som arbetar på uppdrag åt kommunkoncernen, exempelvis konsulter eller inhyrd kompetens.

INLEDNING

EU:s allmänna dataskyddsförordning (2016/679) (”dataskyddsförordningen”), som även kallas GDPR, syftar till att skydda enskilda personer mot kränkning av den personliga integriteten vid behandling av personuppgifter. Förordningen innehåller bland annat regler om när personuppgifter får samlas in, hur de får behandlas och hur registrerade ska informeras. Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, (”dataskyddslagen”), är en svensk nationell lag som kompletterar dataskyddsförordningen.

Dataskyddsförordningen, tillsammans med kompletterande nationella regler, ska tillämpas på all behandling av personuppgifter i kommunkoncernen. Syftet med detta dokument är att ange ansvar och övergripande rutiner när det gäller behandling av personuppgifter i kommunkoncernen. Dataskyddsförordningen är underordnad tryckfrihetsförordningen och yttrandefrihetsgrundlagen och ska därmed inte tillämpas i den utsträckning som den strider mot dessa grundlagar.

VIKTIGA BEGREPP

Personuppgifter: Personuppgifter är varje upplysning som direkt eller indirekt kan knytas till en fysisk person i livet, så som exempelvis namn, adress, personnummer, fingeravtryck, dna, bilder på en person, ljudupptagning av röst med mera. En personuppgift kan även vara en kombination av uppgifter som gemensamt gör att uppgifterna kan knytas till en person.

Behandling av personuppgifter: Med behandling menas varje åtgärd som görs med personuppgifter. Det kan vara att man exempelvis via ett system samlar in, registrerar, läser

av, överför och lagrar personuppgifter. Dataskyddsförordningen gäller för helt eller delvis automatiserad behandling av personuppgifter. Förordningen gäller också för manuell behandling av personuppgifter om personuppgifterna ingår eller är avsedda att ingå i ett manuellt register som är sökbart enligt särskilda kriterier. Ett pappersregister är sökbart om det är sorterat enligt specifika kriterier så som till exempel en pärm där det finns uppgifter om personal sorterat på första bokstaven i efternamnet eller journalhandlingar i ett arkivskåp som är sorterade på födelsedatum.

Personuppgiftsansvarig: Juridisk person, nämnd eller annat bolagsorgan som bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Ansvarsskyldighet: Personuppgiftsansvarig ska kunna visa att dataskyddsförordningen efterlevs och på vilket sätt.

Artikel 30-register: Personuppgiftsansvarig är skyldig att föra register över sina behandlingar av personuppgifter. Vad som ska finnas med i registret beskrivs i art. 30 i dataskyddsförordningen.

Personuppgiftsincident: En säkerhetsincident som leder till förstöring eller förlust av de personuppgifter som behandlas.

Registrerad: Den som personuppgiften avser.

Tillsynsmyndighet: Integritetsskyddsmyndigheten (”IMY”) är tillsynsmyndighet. Registrerad har rätt att lämna in klagomål till IMY om registrerad anser att personuppgifter behandlas i strid med dataskyddsförordningen.

Känsliga personuppgifter: Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd i dataskyddsförordningen. Det är som regel förbjudet att behandla känsliga personuppgifter, men det finns undantag. Innan ni behandlar känsliga personuppgifter måste ni ha klart för er vilket stöd ni har för behandlingen.
Känsliga personuppgifter är uppgifter om:

- etniskt ursprung,
- politiska åsikter, (förtroendevalda anses ha offentliggjort sin politiska åsikt, varför uppgiften kan behandlas enligt undantaget i art. 9 dataskyddsförordningen),
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- hälsa,
- en persons sexualliv eller sexuella läggning,
- genetiska uppgifter,
- biometriska uppgifter som används för att entydigt identifiera en person.

Eftersom känsliga personuppgifter anses ha större skyddsvärde än andra personuppgifter ställs det höga krav på att dessa uppgifter ges ett mer omfattande skydd.

Andra extra skyddsvärda personuppgifter: Det finns många andra typer av personuppgifter som är särskilt skyddsvärda. IMY kallar dessa uppgifter för integritetskänsliga personuppgifter.
Det kan till exempel vara:

- löneuppgifter,
- uppgifter om lagöverträdelser,
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler,
- personuppgifter om barn,
- uppgifter om sociala förhållanden.

Tänk på att integritetskänsliga personuppgifter

- kan kräva en högre säkerhetsnivå än för mer harmlösa personuppgifter,
- har betydelse för riskbedömning när en konsekvensbedömning görs,
- kan vara avgörande för om man måste rapportera en personuppgiftsincident,
- i möjligaste mån inte ska behandlas i e-post eller molntjänster.

Personnummer och samordningsnummer: Personnummer och samordningsnummer räknas inte som känsliga personuppgifter enligt dataskyddsförordningen, men kan anses vara extra skyddsvärda och behöver ofta utökat tekniska säkerhetsåtgärder.

Skyddade personuppgifter: Om någon är utsatt för ett allvarligt hot kan Skatteverket besluta om skyddade personuppgifter i särskilda fall.
Det finns tre typer av skyddade personuppgifter inom folkbokföringen:

1. Sekretessmarkering, lägre grad av skyddade personuppgifter, en varningssignal om skadeprövning.
2. Skyddad folkbokföring, ger ett starkare skydd än sekretessmarkering.
3. Fingerade personuppgifter, personen får ett nytt namn och personnummer.

Den enskilde personen har ett eget ansvar att själv upplysa om skyddade personuppgifter. När det gäller behandling av skyddade personuppgifter ska den personuppgiftsansvarige, utöver att se till att behandlingen följer dataskyddsförordningen, även tänka på följande:

- Regler och rutiner ska finnas för att säkerställa att skydda personuppgifter behandlas på ett sådant sätt att det inte innebär en ökad risk för den registrerade.
- En risk- och konsekvensbedömning ska göras från fall till fall då behovet av vilka personuppgifter som behöver särskilt skydd varierar.
- Endast registrera personuppgifter nödvändiga för ändamålet, dessa ska även gallras så snart de inte längre behövs.
- Åtkomsten till de skyddade personuppgifterna ska begränsas till ett fåtal personer.
- Samtliga medarbetare som kommer i kontakt med skyddade personuppgifter ska få utbildning om de regler och rutiner som gäller.

ANSVAR OCH ORGANISATION

PERSONUPPGIFTSANSVARIG

Varje nämnd och bolag är personuppgiftsansvarig för all behandling av personuppgifter i sin egen verksamhet. Ansvaret kan inte delegeras. Ansvaret gäller såväl personuppgifter om anställda och förtroendevalda som personuppgifter om medborgare, barn, elever, brukare, klienter och kunder. Ansvaret omfattar även personuppgiftsbehandling som sker för kommunkoncernens räkning via ett personuppgiftsbiträde. Personuppgiftsansvaret är omfattande och följande lista tjänar som vägledning för vad som ingår. Listan är inte uttömmande.

Personuppgiftsansvarig ansvarar bland annat för:

- att all personuppgiftsbehandling alltid följer rådande dataskyddslagstiftning,
- att försäkra sig om att förvaltningen och verksamheten har en ändamålsenlig organisation med tillräckliga resurser och dokumenterad ansvarsfördelning,
- att upprätthålla registerförteckning över samtliga personuppgiftsbehandlingar i den ansvariges verksamhet, ett s.k. art 30-register,
- att säkerställa att medarbetarna har nödvändig kompetens för att kunna följa dataskyddslagstiftningen,
- att säkerställa att det tecknas personuppgiftsbiträdesavtal med de leverantörer och motsvarande som behandlar personuppgifter för verksamhetens räkning,
- att säkerställa att personuppgiftsincidenter hanteras i enlighet med dataskyddslagstiftningens krav,
- att utse dataskyddsombud och anmäla dess kontaktuppgifter till tillsynsmyndigheten,
- att stödja dataskyddsombudet i utförandet av de uppgifter som dataskyddsförordningen föreskriver och se till att ombudet har tillräcklig kompetens.

DATASKYDDSOMBUD

Den som är personuppgiftsansvarig ska under vissa givna förhållanden utse ett dataskyddsombud. Ombudets roll är att kontrollera att dataskyddsförordningen följs och att ge råd, stöd och utbildning till organisationen i dataskyddsfrågor. Dataskyddsombudet intar en självständig ställning gentemot personuppgiftsansvarig, som kan jämställas med en internrevisors. Dataskyddsombudet kan inte avsättas eller bli föremål för sanktioner för att ha utfört sina arbetsuppgifter. Dataskyddsombudet är bundet av sekretess inom ramen för sitt uppdrag. Myndigheter och offentliga organ måste alltid ha ett dataskyddsombud.

DATASKYDDSSAMORDNARE

Dataskyddssamordnaren har en samordnande roll i kommunkoncernens övergripande arbete med frågor om personuppgiftsbehandling och dataskydd. Dataskyddssamordnaren är en stödfunktion. Ansvaret för att lagstiftning efterlevs vilar alltid på personuppgiftsansvarig och ansvaret kan inte delegeras.

Dataskyddssamordnaren svarar för interna dataskyddsfrågor och stöttar kontaktpersoner för dataskyddsfrågor genom lämpligtvis men inte uteslutande följande uppgifter:

- hålla sig underrättad om utvecklingen av lagstiftningen och praxis inom området,
- ge råd och stöd till berörd personal i frågor rörande dataskydd,
- följa upp att verksamheten genomför grundutbildning för varje medarbetare och i övrigt följa upp och föreslå kompetensutveckling,
- bidra till utvecklingen av kommunkoncerngemensamma rutiner och arbetssätt,
- löpande följa upp de kommunkoncernövergripande rutinerna för hantering och anmälan av personuppgiftsincidenter är kända i verksamheten
- bistå med stöd och utbildning rörande registerförteckning (art. 30-register),
- vara stöd vid upprättande av personuppgiftsbiträdesavtal
- ge råd vid en konsekvensbedömning avseende dataskydd (DPIA) genomförs,
- vara dataskyddsombudets kontaktperson i dataskyddsfrågor.

KONTAKTPERSONER FÖR DATASKYDDSFRÅGOR

Kontaktpersoner för dataskyddsfrågor är en funktion som ska finnas inom varje förvaltning och bolag. Rollen kan kombineras med andra arbetsuppgifter om det bedöms möjligt. Kontaktpersonen är en stödfunktion. Ansvaret för att lagstiftning efterlevs vilar alltid på personuppgiftsansvarig och ansvaret kan inte delegeras.

Kontaktpersonen stöttar den egna förvaltningen/bolaget genom lämpligtvis men inte uteslutande följande uppgifter:

- löpande uppdatera och följa upp registerförteckningen,
- administrera begäran om registerutdrag,
- administrerar anmälan av personuppgiftsincident
- följa upp att förvaltningen genomför grundutbildning för varje medarbetare
- vara stöd vid upprättande av personuppgiftsbiträdesavtal,
- administrera vid en konsekvensbedömning avseende dataskydd (DPIA) genomförs,
- vara kontaktperson för den egna förvaltningen gentemot dataskyddssamordnare och dataskyddsombudet.

ÖVRIGA CHEFER OCH MEDARBETARE

Samtliga medarbetare har ett ansvar för att behandling av personuppgifter utförs på ett korrekt och lagligt sätt. Riktlinjer, rutiner och arbetsinstruktioner ska vara kända inom organisationen och det åligger varje chef att förmedla vikten av att följa gällande styrdokument.

PRINCIPER FÖR BEHANDLING AV PERSONUPPGIFTER

För att vara laglig ska behandlingen av personuppgifter uppfylla kraven beträffande de grundläggande principerna i dataskyddsförordningen. Art. 5 och art. 6 i dataskyddsförordningen, som behandlar den lagliga grunden, är alltså grundläggande och ska läsas tillsammans. Art. 5 reglerar förutsättningarna för ”hur” personuppgifter får behandlas, medan art. 6 kan beskrivas som att den reglerar ”om” personuppgifter får behandlas. Dessa är de viktigaste grunderna vid behandling av personuppgifter.

Av art. 5 dataskyddsförordningen framgår följande principer för behandling samt ansvarsskyldigheten:

Laglighet, korrekthet och öppenhet: Personuppgifter får enbart behandlas om det finns en laglig grund enligt dataskyddsförordningen. Ställer även krav på att behandlingen inte får vara oskälig.

Ändamålsbegränsning: Personuppgifter ska behandlas för ett särskilt uttryckt, angivet ändamål och de får senare inte behandlas på ett sätt som är oförenligt med ändamålet.

Uppgiftsminimering: Fler personuppgifter får inte behandlas än vad som är nödvändigt och relevant med hänsyn till ändamålet. Personuppgifter ska inte behandlas för att de kan vara ”bra att ha”.

Korrekthet: Behandling av personuppgifter ska vara korrekt i förhållande till ändamålet. Personuppgifter som är felaktiga ska rättas eller raderas utan dröjsmål.

Lagringsminimering: Ändamålet avgör hur länge personuppgifter får lagras. Kommunkoncernen har dock rättslig förpliktelse att spara en del uppgifter enligt arkivlagen och detta regleras i nämndernas och bolagens dokumenthanteringsplaner.

Integritet och konfidentialitet: Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av tekniska och organisatoriska åtgärder. Lämplig säkerhet beror på riskerna som är förknippade med behandlingen.

Ansvarsskyldighet: Personuppgiftsansvarig ska kunna visa att dataskyddsförordningen efterlevs och på vilket sätt. Dokumentation och en god ordning på dokument samt diarieföring enligt rutiner och lagregler är en viktig del av ansvarsskyldigheten. Vid en begäran av tillsynsmyndigheten ska personuppgiftsansvarig kunna visa upp sin dokumentation och specifikt ett s.k. art. 30-register.

LAGLIG GRUND FÖR BEHANDLING AV PERSONUPPGIFTER

Personuppgifter får endast behandlas om ett av följande villkor är uppfyllt enligt art. 6 dataskyddsförordningen.

UTFÖRA EN UPPGIFT AV ALLMÄNT INTRESSE ELLER MYNDIGHETSUTÖVNING

Personuppgifter får behandlas om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse. För att en uppgift ska anses vara av allmänt intresse ska uppgiften ha stöd i lag eller annan författning t.ex. tryckfrihetsförordningen, arkivlagen, skollagen etc.

Den lagliga grunden myndighetsutövning innebär att personuppgiftsbehandling är tillåten om ni behandlar personuppgifter i er myndighetsutövning. All myndighetsutövning ska grundas på lagar, förordningar eller andra författningar.

FULLGÖRA ETT AVTAL

Personuppgifter får behandlas om det är nödvändigt för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige.

FULLGÖRA EN RÄTTSLIG FÖRPLIKTELSE

Personuppgifter får behandlas om det till exempel anges i lag att den personuppgifts-ansvarige är skyldig att lämna vissa uppgifter till en annan myndighet eller till en domstol, ex. bokföringsskyldighet enligt bokföringslagen eller att kommunens nämnder, i egenskap av arbetsgivare, är skyldiga att redovisa skatter och sociala avgifter avseende sina anställda.

SKYDDA GRUNDLÄGGANDE INTRESSEN

Personuppgifter får behandlas om det är nödvändigt för att rädda en persons liv. I huvudsak handlar det om tillfällen när personen inte kan fatta beslut eller lämna samtycke, till exempel om en person är medvetslös.

SAMTYCKE

Personuppgifter får behandlas om den registrerade ger sitt uttryckliga samtycke till behandlingen. Ett lämnat samtycke kan alltid återkallas.

Ett samtycke kan inte användas som laglig grund för behandling av personuppgifter i fall där det råder betydande ojämlikhet mellan den registrerade och personuppgiftsansvariga. Kommunen har därför begränsade möjligheter att använda sig av samtycke som laglig grund och bör hitta en annan laglig grund. Samtycke är även olämpligt i anställningsförhållanden eftersom anställda står i beroendeställning till arbetsgivaren.

UTFÖRA EN INTRESSEAVVÄGNING

Det kan vara tillåtet att behandla personuppgifter efter en intresseavvägning. Myndigheter kan inte stödja sin behandling av personuppgifter på en intresseavvägning. Kommunen kan alltså inte behandla personuppgifter med stöd av en intresseavvägning.

DEN REGISTRERADES RÄTTIGHETER

Den registrerade har ett antal rättigheter enligt dataskyddsförordningen. Dessa rättigheter innebär i korthet att den registrerade ska få information om när och hur dennes personuppgifter behandlas och kunna ha kontroll över sina egna uppgifter. Därför har den registrerade bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller blockerade (begränsade).

RÄTT TILL TILLGÅNG (BEGÄRAN AV REGISTERUTDRAG)

Den registrerade har rätt att få information om huruvida personuppgifter som rör denne behandlas och i så fall få tillgång till personuppgifterna. En begäran kan göras skriftligen eller digitalt i en av kommunen särskilt framtagen e-tjänst för detta ändamål. Den personuppgiftsansvarige ska lämna ett skriftligt besked till den registrerade inom en månad från det att begäran kom in. Det skriftliga beskedet ska lämnas i e-tjänsten eller genom skriftligt brev till den registrerades folkbokföringsadress.

RÄTT TILL RÄTTELSE

Den registrerade har rätt att få felaktiga personuppgifter rättade. Det innebär också att den registrerade har rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen.

RÄTT TILL RADERING ("RÄTTEN ATT BLI GLÖMD")

Om den registrerade begär att bli bortglömd är personuppgiftsansvarig skyldig att radera personuppgifterna i vissa särskilda fall. Rätten att bli bortglömd är dock mycket begränsad i en myndighets verksamhet. Exempelvis kan det krävas att personuppgifterna sparas för att uppfylla lagstiftningens krav på bevarande av allmänna handlingar, för att kommunen ska kunna utföra en uppgift av allmänt intresse eller som ett led i kommunens myndighets-utövning.

ÖVRIGA RÄTTIGHETER

Den registrerade har i vissa fall rätt att begära att få ut sina uppgifter i ett allmänt läsbart format (rätt till dataportabilitet), att begära att personuppgiftsbehandlingen begränsas (rätt till begränsning) och rätt att göra invändningar mot personuppgiftsbehandlingen. Den registrerade kan lämna klagomål som avser behandling av personuppgifter till person-uppgiftsansvarig, dataskyddsombudet eller tillsynsmyndigheten.

SÄKERHET VID BEHANDLING

Den personuppgiftsansvarige är skyldig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas i verksamheten. I det arbetet ingår att kartlägga integritetsrisker och ha rutiner för upptäckt och hantering av personuppgiftsincidenter. Det är viktigt att vidta säkerhetsåtgärder för att skydda de personuppgifter som hanteras inom verksamheten. Säkerhetsarbetet ska även omfatta personuppgifter om anställda.

Vilka säkerhetsåtgärder som är lämpliga beror bland annat på hur känslig behandlingen är, vilka risker som finns för de anställda och vilka tekniska lösningar som är tillgängliga.

TEKNISKA SÄKERHETSÅTGÄRDER

Exempel på tekniska säkerhetsåtgärder är inloggning med stark autentisering, behörighetsspärrar, loggar, brandväggar, kryptering, pseudonymisering, säkerhetskopiering och antivirusskydd.

ORGANISATORISKA SÄKERHETSÅTGÄRDER

Organisatoriska säkerhetsåtgärder handlar om det administrativa säkerhetsarbetet som till exempel tilldelning av åtkomsträttigheter, interna regler och rutiner, instruktioner, riktlinjer, och policydokument. Utbildning är en viktig del av det organisatoriska säkerhetsarbetet.

För att bedöma vilka säkerhetsåtgärder som är lämpliga måste den personuppgiftsansvarige göra en helhetsbedömning av vilka risker som behandlingen innebär i det enskilda fallet. Även behandling av känsliga personuppgifter kan ha olika risknivå beroende på i vilket sammanhang behandlingen förekommer, hur ingripande behandlingen är och på vilket sätt den genomförs.

INBYGGT DATASKYDD (PRIVACY BY DESIGN)

Inbyggt dataskydd (privacy by design) innebär att man tar hänsyn till integritetsskydds-reglerna redan när man utformar it-system och rutiner. Det är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas. Principen om inbyggt dataskydd bör alltid beaktas vid inköp och upphandling och under hela IT-systemets livscykel.

DATASKYDD SOM STANDARD (PRIVACY BY DEFAULT)

Kravet på dataskydd som standard (privacy by default) innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i en tjänst för sociala media är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas.

ÖVERFÖRING TILL TREDJE LAND

Överföring av personuppgifter till tredje land är när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området (så kallad tredjelandsöverföring) och är enligt huvudregeln i art. 44 dataskyddsförordningen förbjudet.

För överföring av personuppgifter till länder utanför EU/EES-området gäller särskilda undantagsregler. Dataskyddsförordningen innebär att alla EU:s medlemsstater samt EES-länderna har ett likvärdigt skydd för personuppgifter och personlig integritet och därför kan personuppgifter föras över fritt inom det området utan begränsningar. För länder utanför det området finns däremot inte några generella regler som ger motsvarande garantier och därför får tredjelandsöverföring endast ske under särskilda förutsättningar. Det här berör varje form av överföring av information över gränserna, t.ex. många online IT-tjänster, molnbaserade tjänster, appar, tjänster för extern åtkomst eller globala databaser m.m. och behöver analyseras särskilt.

Exempel på överföring av personuppgifter till tredje land:

- När personuppgifter behandlas i en molntjänst (ex. Microsoft Azure, Google Cloud, Amazon Web Services) som är baserad utanför EU/EES, via e-post, chattkonversationer, appar och filer som lagras på olika delningsytor
- När ett personuppgiftbiträde anlitas i ett land utanför EU/EES.
- När någon utanför EU/EES får tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES.
- När personuppgifter lagras, till exempel på en server, i ett land utanför EU/EES.

Att publicera något på internet är inte tredjelandsöverföring om webbplatsen lagras hos en internetleverantör som är etablerad inom EU.

ADEKVAT SKYDDSNIVÅ

EU-kommissionen kan fatta beslut om att ett land har en tillräckligt hög skyddsnivå och personuppgiftsansvarig får då föra över personuppgifter dit på ett lagligt sätt. I dataskyddsförordningen kallas det för adekvat skyddsnivå. När EU-kommissionen fattar beslut om adekvat skyddsnivå tittar de bland annat på landets lagar och internationella åtaganden, vilka möjligheter den registrerade har att få rättslig prövning och om landet respekterar de mänskliga rättigheterna och de grundläggande friheterna. EU-kommissionen kontrollerar också att det finns oberoende tillsynsmyndigheter som ansvarar för att dataskyddsreglerna följs och som kan hjälpa den registrerade. Den personuppgiftsansvarige får inte själv avgöra om det finns en adekvat skyddsnivå eller inte. Det är bara EU-kommissionen som kan fatta ett sådant beslut.

EU-kommissionen har fattat beslut om att skyddsnivån i dessa länder är adekvat, det vill säga tillräckligt hög enligt dataskyddsförordningen:
Andorra, Argentina, Baliwick of Guernsey, Färöarna, Isle of Man, Israel, Japan, Jersey, Nya Zeeland, Schweiz, Storbritannien, Sydkorea, Uruguay samt Kanada.

Överenskommelsen med USA, Privacy Shield, ogiltigförklarades av EU-domstolen den 16 juli 2020 och kan inte längre användas vid överföring av personuppgifter mellan EU och USA. Nya beslut fattas löpande och uppgifterna ska kontrolleras hos IMY vid behov.

NÄR FÅR UPPGIFTER ANNARS ÖVERFÖRAS TILL TREDJE LAND?

Personuppgifter får överföras till ett land utanför EU/EES om det bland annat finns godkända standardavtalsklausuler.

STANDARDAVTALSKLAUSULER (SCC)

EU-kommissionen har godkänt vissa standardavtalsklausuler som handlar om dataskydd (Standard Contractual Clauses, SCC). Den senaste versionen godkändes av EU-kommissionen den 4 juni 2021. Om avtal ingås, som innehåller dessa standardavtals-klausuler, med någon utanför EU/EES, är det tillåtet att överföra personuppgifter till dem. Observera dock att man inte får ändra i klausulerna. Standardavtalsklausulerna innehåller skyldigheter dels för personuppgiftsansvariga som vill föra över personuppgifter till länder utanför EU/EES, dels för personuppgiftsansvariga eller personuppgiftsbiträden som tar emot sådana uppgifter. Klausulerna återspeglar också de krav på tredjelandsöverföring som uppställs i dataskyddsförordningen med exempel på tekniska och organisatoriska skyddsåtgärder och tar hänsyn till följderna av den så kallade Schrems II-domen (EU-domstolen nr C-311/18). Enligt rekommendationer från Europeiska Dataskyddsstyrelsen (”EDPB”) måste standardavtalsklausulerna kompletteras med ytterligare tekniska och organisatoriska skyddsåtgärder för att nå adekvat skyddsnivå.

KONSEKVENSBEDÖMNING

Den personuppgiftsansvarige måste i vissa fall göra en konsekvensbedömning avseende dataskydd vid behandling av personuppgifter som innebär förhöjda integritetsrisker. I dessa fall ska dataskyddsombudet rådfrågas. En konsekvensbedömning avseende dataskydd kräver att personuppgifterna klassificeras utifrån såväl dataskyddslagstiftning och offentlighets- och sekretesslagen som utifrån informationssäkerhet. Klassning och konsekvensbedömning ligger till grund för vilka säkerhetskrav som ska ställas på organisatoriska och tekniska säkerhetslösningar samt på fysisk säkerhet. Om en personuppgiftsbehandling sannolikt leder till en hög risk för de registrerades rättigheter och friheter är den personuppgiftsansvarige skyldig att göra en konsekvensbedömning.
IMY kan i förhandssamråd utfärda råd, förelägganden eller förbud som säkerställer att behandlingen är i enlighet med dataskyddsförordningens regler.

PERSONUPPGIFTSINCIDENTER

En personuppgiftsincident är en säkerhetsincident som innebär att personuppgifter oavsiktligt eller olagligt förstörs, förloras, ändras eller röjs. Det kan även handla om att någon får obehörig åtkomst till de personuppgifter som behandlas. Kommunkoncernen har en e-tjänst samt rutin för rapportering av misstänkta och/eller inträffade personuppgifts-incidenter.

Respektive nämnd och bolag ansvarar för att dess anställda är medvetna om sin skyldighet att rapportera personuppgiftsincidenter i e-tjänsten enligt de rutiner som gäller.

Personuppgiftsincidenter ska anmälas till IMY såvida det inte är osannolikt att incidenten kommer innebära risker för de registrerade. En sådan anmälan ska göras inom 72 timmar från det att någon i organisationen fick kännedom om incidenten. Det är därför mycket viktigt att incidenten rapporteras omgående i e-tjänsten. I vissa fall ska nämnden också informera den registrerade om incidenten.

PERSONUPPGIFTER I ALLMÄNNA HANDLINGAR

Kommunkoncernen behandlar en stor mängd personuppgifter i handlingar. Det ligger på respektive nämnd och bolag att hantera brev eller e-post som innehåller personuppgifter på ett säkert sätt, såsom i säkra ärendehanteringssystem.

Enligt dataskyddsförordningen får kommunkoncernen, för att utföra en uppgift av allmänt intresse, lämna ut personuppgifter i allmänna handlingar i enlighet med offentlighets-principen. Skyldigheten att lämna ut allmänna handlingar enligt offentlighetsprincipen gäller dock inte elektronisk utlämning av handlingar. Dataskyddsförordningen gäller därför för de handlingar som lämnas ut via e-post eller via e-tjänster. De som begär ut allmänna handlingar har enligt offentlighetsprincipen endast en rätt att läsa uppgifterna på plats eller få en fysisk kopia av handlingarna. De personuppgifter som lämnas ut elektroniskt måste därför skyddas genom lämpliga skyddsåtgärder enligt dataskyddsförordningen.

hantering av personuppgifter i e-post

E-post innehåller nästan alltid personuppgifter, till och med själva e-postadressen är i sig en personuppgift, det betyder att dataskyddsförordningen gäller för e-post. Det ligger på respektive nämnd och bolag att hantera brev eller e-post som innehåller personuppgifter på ett säkert sätt, såsom i säkra ärendehanteringssystem. För att inte sprida personuppgifter försök att i möjligaste mån styra bort att hantera personuppgifter i e-post, använd istället avsedda ärendehanteringssystem.

INKOMMEN E-POST

Det som skiljer e-post från annan uppgiftshantering är att innehållet oftast är okänt när e-posten kommer in till verksamheten. Utgångspunkten är att en verksamhet behöver ta hand om inkommande post. Myndigheter kan därför som regel behandla personuppgifter i e-post med stöd av den lagliga grunden att utföra en uppgift av allmänt intresse.

När e-posten väl är mottagen beror det på innehållet om och hur länge det får sparas. Personuppgifter som ska fortsätta behandlas ska överföras till ett ärendehanteringssystem och sedan ska e-postmeddelandet raderas. Känsliga personuppgifter, integritetskänsliga personuppgifter eller sekretessbelagda uppgifter som kommit in oskyddade via e-post ska raderas ur ett e-postsvar eller vid vidarebefordran.

Offentlighetsprincipen går före dataskyddsförordningen men dataskyddsförordningen styr hur uppgifterna lämnas ut. Kommunkoncernen är inte skyldig att lämna ut uppgifter i elektronisk form via e-post, tryckfrihetsförordningen reglerar enbart utlämning per post eller möjligheten att ta del av handlingen på stället.

E-post som kommer in till kommunkoncernen blir normalt en allmän handling som ska registreras eller hållas ordnad. Kommunkoncernen är enligt arkivlagen skyldig att bevara allmänna handlingar. Utgångspunkten är att det är tillåtet att behandla personuppgifter för att uppfylla kraven i arkivlagen om bevarande av allmänna handlingar. Alla e-post-meddelanden hos myndigheter är dock inte allmänna handlingar, till exempel privata meddelanden och meddelanden inom en facklig organisation.

FLYTTA PERSONUPPGIFTER FRÅN E-POSTEN

Det är tillåtet för kommunen som myndighet att ta emot personuppgifter via e-post, men e-postsystemet ska inte användas för att spara uppgifter under en längre tid eftersom det inte är en säker lagringsplats. Personuppgifter som inkommit via e-post ska istället flyttas från e-posten till ett lämpligare system, som till exempel ett ärendehanteringssystem.

FÖRHINDRA ATT PERSONUPPGIFTER SPRIDS

Sprid inte personuppgifter i onödan. Skicka bara personuppgifter till dem som behöver uppgifterna för sitt arbete. Om e-post måste användas, undersök om det går att avidentifiera uppgifterna. Om du skickar e-post till många samtidigt, överväg om adresserna ska skrivas i fältet för dold kopia. Undvik att skicka e-postmeddelanden som kopia i onödan.

Undvik att bifoga dokument som innehåller personuppgifter. Spara istället dokumentet på ett ställe och skicka en länk till dokumentet via e-post.

KÄNSLIGA PERSONUPPGIFTER FÅR INTE BEHANDLAS I E-POST

Känsliga personuppgifter och uppgifter under sekretess får inte skickas via e-post. I möjligaste mån ska det undvikas att behandla integritetskänsliga personuppgifter och extra skyddsvärda personuppgifter via e-post. Om ni måste använda e-post för integritetskänsliga personuppgifter, använd e-post som är skyddad med kryptering så att endast den avsedda mottagaren kan ta del av uppgifterna.

Försök att i möjligaste mån styra bort att enskilda skickar in känsliga personuppgifter via oskyddad e-post. Om ni får in känsliga personuppgifter via e-post, se till att de tas bort från e-posten så snart som möjligt. Ange inte heller känsliga personuppgifter i ditt autosvar, såsom uppgift om din sjukfrånvaro.

UNDVIK PERSONUPPGIFTER I RUBRIKRADEN

Skriv inte namn på personer i ämnesraden på e-postmeddelandet. Skriv inte heller några andra integritetskänsliga personuppgifter som till exempel uppgifter om hälsa eller personnummer.

SKAPA MALLAR FÖR ÅTERKOMMANDE UTSKICK

Låt inte e-post ligga kvar i e-postlådan för framtida bruk av formuleringar. Sådana texter bör istället tömmas på personuppgifter och göras om till mallar som sparas på annan plats.

PUBLICERING AV PERSONUPPGIFTER DIGITALT

PUBLICERING AV ANSTÄLLDAS OCH FÖRTROENDEVALDAS PERSONUPPGIFTER

Publicering av anställdas personuppgifter, såsom namn, befattning, kommunalt telefonnummer och kommunal e-postadress och liknande arbetsplatsrelaterade personuppgifter kan normalt publiceras utan den registrerades samtycke om publiceringen är nödvändig för att informera om kommunkoncernens verksamhet. Den lagliga grunden för publiceringen är i sådant fall utföra uppgift av allmänt intresse. Uppgifter om familjeförhållanden, bostadsadress, privat telefonnummer och fritidsintressen får inte publiceras.

Publicering av förtroendevaldas personuppgifter, såsom namn, parti och kommunal e-postadress som tillhandahålls av kommunkoncernen får publiceras med stöd av den lagliga grunden utföra uppgift av allmänt intresse. Partitillhörighet är en känslig personuppgift enligt dataskyddsförordningen men med hänsyn till att förtroendevalda anses ha offentliggjort sin politiska åsikt kan uppgiften behandlas enligt undantaget i art. 9 dataskyddsförordningen. Den förtroendevaldes privata telefonnummer eller privata e-postadress ska inte publiceras. Uppgifter om förtroendevaldas familjeförhållanden, bostadsadress, privat telefonnummer och fritidsintressen får inte publiceras.

PUBLICERING AV FOTO OCH FILM PÅ KOMMUNKONCERNENS ANSTÄLLDA

Möjligheten att publicera foto och film på anställda får bedömas i varje enskilt fall. Att få sin bild publicerad på internet kan av många upplevas som särskilt känsligt. Samtycke är ofta inte lämpligt i anställningsförhållande eftersom anställda står i beroendeställning till arbetsgivaren, man måste alltså hitta en annan laglig grund. Om ändamålet är att informera om verksamheten kan den lagliga grunden vara att behandlingen är nödvändig för att uppfylla en uppgift av allmänt intresse.

Ett alternativ är att ingå ett modellavtal med den anställde och publiceringen stöds då av den lagliga grunden att behandlingen är nödvändig för att fullgöra ett avtal.

PUBLICERING AV FOTO OCH FILM PÅ MEDBORGARE

Publicering av foto och film för att informera om kommunkoncernens verksamhet:
Vid syftet med att publicera foto och film av medborgare för att informera om kommunkoncernens verksamhet kan den lagliga grunden vara att kommunkoncernen utför en uppgift av allmänt intresse när foto och film publiceras. Att det är en myndighets uppgift att tillhandahålla information om sin verksamhet framgår av 6 § myndighetsförordningen.

PUBLICERING AV PERSONUPPGIFTER I PROTOKOLL OCH DIARIER

Kommunkoncernen får publicera information på internet från vissa allmänna handlingar även om informationen omfattar personuppgifter (harmlösa). De allmänna handlingar som avses är sådana som utgör eller ingår i:

- diarium (som avses i 5 kap. 2 § offentlighets- och sekretesslagen)
- kallelse till ett sammanträde med fullmäktige eller nämnd
- kungörelse om sammanträde med fullmäktige, eller
- justerat protokoll som har förts vid ett sammanträde med fullmäktige eller en nämnd.

PERSONUPPGIFTER SOM INTE FÅR PUBLICERAS

Följande personuppgifter får inte publiceras på kommunkoncernens webbplats:

- Uppgifter som omfattas av sekretess och tystnadsplikt
- Känsliga personuppgifter
  - Uppgifter som avslöjar politiska åsikter och medlemskap i fackförening får publiceras i de fall som den enskilde själv på ett tydligt sätt offentliggjort uppgifterna (till exempel förtroendevalda politikers politiska åsikter eller fackliga företrädares medlemskap i fackförening).
- Integritetskänsliga personuppgifter, till exempel uppgifter om enskildas personliga förhållanden eller sådant som har en nära koppling till den enskildes privata sfär
- Personnummer eller samordningsnummer

RÄTTSLIGA KONSEKVENSER

Ansvaret för behandling av personuppgifter ligger alltid på den personuppgiftsansvarige. IMY är tillsynsmyndighet. IMY kan i vissa fall döma ut en administrativ sanktionsavgift till följd av överträdelser av dataskyddslagstiftningen. Sanktionsavgiften för myndigheter kan som mest uppgå till 10 miljoner kronor per överträdelse.

Varje person som lidit skada till följd av överträdelser av dataskyddsförordningen har rätt till skadestånd av personuppgiftsansvarige för den uppkomna skadan.