Riktlinjer för behandling av personuppgifter

PROGRAM PLAN POLICY **RIKTLINJER**

Helsingborgs stads styrdokument

Aktiverande
syftar till förändring och utveckling

PROGRAM – anger långsiktiga ambitioner och viljeinriktningar
PLAN – anger konkreta åtgärder, tidsramar och ansvar

Normerande
reglerar befintlig verksamhet och vårt förhållningssätt till en given situation

POLICY – anger principer och vägledning
RIKTLINJE – anger absoluta gränser och ska-krav

Beslutat av: Kommunstyrelsen
Datum: 12 februari 2020, § 29
Dokumentet gäller för: Alla nämnder och förvaltningar
Dokumentansvarig: Stadsledningsförvaltningens avdelning för juridik och administration

HELSINGBORG

Innehållsförteckning

HELSINGBORG

1 Inledning

EU:s dataskyddsförordning (2016/679), 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, som även kallas dataskyddslagen, är en nationell lag som kompletterar förordningen.

EU:s dataskyddsförordning (dataskyddsförordningen), tillsammans med kompletterande nationella regler, ska tillämpas på all behandling av personuppgifter i Helsingborgs stad. Syftet med detta dokument är att ange ansvar och övergripande rutiner när det gäller behandling av personuppgifter i Helsingborgs stad.

Dataskyddsförordningen är underordnad tryckfrihetsförordningen och yttrandefrihetsgrundlagen och ska därmed inte tillämpas i den utsträckning som den strider mot dessa grundlagar. Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från dataskyddslagen, tillämpas den bestämmelsen.

1.1 Viktiga begrepp

1.1.1 Personuppgift

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.

1.1.2 Känsliga personuppgifter

Känsliga personuppgifter (även kallade särskilda kategorier av personuppgifter) är personuppgifter som avser hälsa, sexualliv, biometriska uppgifter[1], ras/etniskt ursprung, politiska åsikter, religiös/filosofisk övertygelse eller medlemskap i fackförening.

1.1.3 Behandling av personuppgifter

Med behandling avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter. Det kan handla om att uppgifter om en person till exempel samlas in, registreras, lagras, bearbetas eller sammanställs.

---

[1] Biometriska uppgifter rör en persons fysiska, fysiologiska eller beteendemässiga egenskaper och gör det möjligt att identifiera människor, till exempel genom fingeravtrycksavläsning eller ögonskanning. Foton på människor är bara biometriska uppgifter när de behandlas med teknik som möjliggör identifiering eller autentisering av en person, till exempel med ansiktsigenkänningsteknik.

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.

1.1.4 Den registrerade

Den person vars personuppgifter behandlas.

1.1.5 Personuppgiftsansvarig

Personuppgiftsansvarig är en fysisk (privatperson) eller juridisk person (företag, förening, stiftelse) eller myndighet som bestämmer för vilka ändamål personuppgifterna ska behandlas och hur behandlingen ska gå till. Den som är personuppgiftsansvarig är ytterst ansvarig för att regelverket följs och att uppgifter om registrerade personer behandlas korrekt.

I Helsingborg stad är varje nämnd personuppgiftsansvarig för den behandling av personuppgifter som sker i respektive nämnds verksamhet.

I dessa riktlinjer används konsekvent begreppet *personuppgiftsansvarig*. Med detta avses respektive nämnd i organisationen.

1.1.6 Personuppgiftsbiträde

Ett personuppgiftsbiträde är en fysisk eller juridisk person som hanterar personuppgifter för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Det kan till exempel vara en leverantör av ett system eller en digital tjänst, så som ett ekonomisystem, verksamhetssystem, en app eller liknande.

1.1.7 Personuppgiftsbiträdesavtal

Den som är personuppgiftsansvarig ansvarar för att det finns ett skriftligt avtal med personuppgiftsbiträdet om den behandling av personuppgifter som biträdet ska genomföra. Det kallas personuppgiftsbiträdesavtal.

Staden har tagit fram en mall för personuppgiftsbiträdesavtal. Aktuell version av mallen finns att hämta på intranätet. Stadens egen mall för biträdesavtal bör användas i första hand. Om biträdet vill använda ett eget avtal är det viktigt att granska avtalet så att det uppfyller lagstiftningens krav på innehåll.

1.1.8 Register över personuppgiftsbehandlingar

Den personuppgiftsansvarige är skyldig att föra ett register över den personuppgiftsbehandling som utförs under dennes ansvar. Registret ska bland annat innehålla uppgift om ändamålet för behandlingen, kategorier av registrerade och personuppgifter, uppgift om mottagare av personuppgifterna med mera.

Staden har tagit fram en e-tjänst som ett verktyg för att anmäla den personuppgiftsbehandling som sker hos respektive nämnd i Helsingborgs stad. I e-tjänsten skapas en förteckning över de personuppgiftsbehandlingar som finns.

Exempel på behandlingar av personuppgifter som ska anmälas:

- Olika verksamhetsspecifika IT-stöd som innehåller personuppgifter.
- Listor i Word och Excel med personuppgifter som till exempel lagras på H eller G (listor för mailutskick och nyhetsbrev, kaffelista, listor med kontaktuppgifter, statistikuttag, listor som lyfts ut från andra IT-stöd och sparats på H eller G med mera).
- Pappersregister som innehåller personuppgifter, om det är ett sökbart register.

Instruktion för att anmäla personuppgiftsbehandling i e-tjänsten finns i bilaga 1.

Observera att om flera register i en verksamhet har samma innehåll och samma ändamål så kan en gemensam anmälan göras för samtliga dessa register. Ändamålet kan dock inte definieras alltför brett för att detta ska vara tillåtet. Exempel på en gemensam anmälan är en anmälan där ändamålet (tänk syftet med personuppgiftsbehandlingen) anges vara register för personaladministration och där deltagarlistor finns för olika arrangemang så som till exempel julfest, lista för friskvårdsbidrag och kaffelista ingår.

Om personuppgifter tillkommer i ett IT-stöd eller en manuell lista som redan har anmälts behöver en ny anmälan inte göras förutsatt att ändamål, kategorier av personer och typ av personuppgifter inte ändras.

1.1.9 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 och stöd till organisationen i dataskyddsfrågor.

Ett dataskyddsombud ska utses på grundval av yrkesmässiga kvalifikationer och sakkunskap om lagstiftning och praxis om dataskydd samt förmågan att fullgöra de uppgifter som följer av dataskyddsförordningen.

1.1.10 Personuppgiftsincident

En personuppgiftsincident är en incident som innebär att personuppgifter oavsiktligt eller olagligt förstörs, förloras, ändras eller till exempel röjs. Det kan även handla om att någon får obehörig åtkomst till de personuppgifter som behandlas.

För mer information om personuppgiftsincidenter och hur de ska hanteras se nedan i avsnitt 6.4.

2 Principer för behandling av personuppgifter

Vid all behandling av personuppgifter ska följande principer tillämpas.

2.1 Behandlingen ska vara laglig

All personuppgiftsbehandling ska vara laglig. Det innebär först och främst att det ska finnas en rättslig grund för all personuppgiftsbehandling som sker. I dataskyddsförordningen finns sex rättsliga grunder, varav en alltid ska vara uppfylld för varje personuppgiftsbehandling som sker i Helsingborgs stad (se mer under avsnitt 3 nedan).

Att behandlingen ska vara laglig innebär också att övriga principer och bestämmelser i dataskyddslagstiftningen och annan lagstiftning ska följas.

2.2 Behandlingen ska vara korrekt

All personuppgiftsbehandling ska vara korrekt. Det innebär att den ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till de registrerade.

Verksamheten ska se till att den personuppgiftsbehandling som sker står i rimlig proportion till den nytta som den innebär och hänsyn ska tas till vad den registrerade kan förvänta sig. Personuppgiftsbehandlingen ska vara förståelig och begriplig för de registrerade och inte ske på dolda eller manipulerande sätt.

2.3 Öppenhet och information till registrerade

Det ska vara klart och tydligt för de registrerade hur verksamheten behandlar personuppgifter. De registrerade ska få reda på om och varför personuppgifter samlas in och hur personuppgifterna sedan används. De registrerade ska också få information om sina rättigheter, så som rätten att begära registerutdrag eller få uppgifter rättade (se vidare nedan i avsnitt 4).

2.4 Begränsa ändamålet med behandlingen

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål (syften). Ändamålet med en personuppgiftsbehandling ska stå klart innan personuppgifterna samlas in och får inte vara allt för opreciserat eller omfattande. Ändamålen sätter ramarna för hur personuppgifterna får behandlas. Personuppgifter får efter insamling inte behandlas för något ändamål som är oförenligt med det ursprungliga ändamålet.

2.5 Uppgiftsminimering

Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet med behandlingen. Det innebär att verksamheten inte ska behandla fler personuppgifter än vad som behövs och att de personuppgifter som behandlas ska vara tydligt kopplade till ändamålet. Det alltså inte är tillåtet att samla in personuppgifter enbart för att de kan vara "bra att ha" i framtiden.

2.6 Riktighet

De personuppgifter som behandlas ska vara riktiga och vid behov uppdaterade.

2.7 Lagringsminimering

Personuppgifter ska bara sparas så länge som uppgifterna behövs med hänsyn till ändamålet med personuppgiftsbehandlingen. Radering och arkivering ska ske i enlighet med den dokumenthanteringsplan som gäller för respektive nämnd.

Det kan vara tillåtet att lagra personuppgifter, även efter att det ursprungliga ändamålet med personuppgiftsbehandlingen slutar att vara aktuellt. Detta gäller om det sker för till exempel arkivändamål av allmänt intresse eller statistiska ändamål.

2.8 Integritet och konfidentialitet

Verksamheten ska se till att de personuppgifter som behandlas skyddas på ett bra sätt genom att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder. Verksamheten måste skydda personuppgifterna mot till exempel obehörig åtkomst, förstöring eller förlust.

Exempel på skyddsåtgärder är brandväggar, kryptering, pseudonymisering, säkerhetskopiering och anti-virus-skydd. Det kan också handla om att det upprättas interna rutiner, instruktioner och riktlinjer för den personuppgiftsbehandling som genomförs.

2.9 Ansvarsskyldighet

Den personuppgiftsansvarige ska se till att ovanstående principer följs och ska också kunna visa att de följs samt på vilket sätt.

3 Rättslig grund för behandling av personuppgifter

Personuppgifter får endast behandlas om det finns rättslig grund för behandlingen. Den rättsliga grunden ska fastställas innan behandling påbörjas enligt någon av nedan punkter.

De rättsliga grunder som oftast är aktuella för Helsingborg stad att använda sig av är avtal (3.1), rättslig förpliktelse (3.2) samt myndighetsutövning och allmänt intresse (3.3).

3.1 Avtal

Personuppgifter får behandlas om en person, om denne har ett avtal med eller ska ingå ett avtal med den personuppgiftsansvarige.

Exempel 1: Stadens nämnder får i egenskap av arbetsgivare behandla personuppgifter om sina anställda för att kunna uppfylla anställningsavtal, till exempel för löneberäkning, registrering av sjukfrånvaro eller i ett flextidssystem.

Exempel 2: Kulturskolan får för att kunna fullgöra ett avtal med sina elever behandla, till exempel namn och adressuppgifter, för att kunna tillhandahålla musikundervisning eller skicka fakturor.

3.2 Rättslig förpliktelse

Personuppgifter får behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som framgår av lag eller annan författning, av kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning.

Den rättsliga förpliktelsen kan exempelvis vara utformad så att det i lag anges att kommunen är skyldig att lämna vissa uppgifter till en annan myndighet eller till en domstol. Det är då tillåtet för kommunen att behandla sådana personuppgifter om registrerade som är nödvändiga för att kunna uppfylla denna uppgiftsskyldighet.

Exempel på sådana förpliktelser:

- Bokföringsskyldigheten som anges i bokföringslagen.
- Stadens nämnder är i egenskap av arbetsgivare skyldiga att redovisa skatter och sociala avgifter beträffande sina anställda.

3.3 Myndighetsutövning och uppgift av allmänt intresse

Personuppgifter får behandlas om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

För att en uppgift ska anses vara av allmänt intresse ska uppgiften ha stöd i lag eller annan författning, i kollektivavtal eller i beslut som har meddelats med stöd av lag eller annan författning.

Uppgifter som kommunen ålagts att utföra genom lag (obligatoriska uppgifter) är av allmänt intresse. Kommuner har också en vidsträckt möjlighet att göra frivilliga åtaganden. Sådana frivilliga åtaganden kan också utgöra uppgifter av allmänt intresse. Som exempel på uppgifter som kommuner utför på frivillig grund men som är av allmänt intresse anges på Datainspektionens hemsida bland annat tillhandahållande av bostäder och fritids- och idrottsanläggningar samt åtgärder för att främja ortens näringsliv och annan kulturell verksamhet.

3.4 Berättigade (grundläggande) intresse

Det är också tillåtet för en personuppgiftsansvarig att behandla personuppgifter om det är nödvändigt för att rädda den registrerades eller någon annan persons liv. Det kallas att skydda intressen som är av grundläggande betydelse. I huvudsak handlar det om tillfällen när den registrerade inte kan fatta beslut eller lämna samtycke, till exempel om en person är medvetslös.

Exempel: En person har plötsligt blivit sjuk och förlorat medvetandet. Vård och räddningstjänst får då behandla personuppgifter för att kontrollera blodgrupp och sjukdomshistoria och för att kontakta anhöriga.

Observera att den här rättsliga grunden endast kan användas i mycket begränsad omfattning, den gäller exempelvis inte om den aktuella vårdinsatsen är planerad (då är en annan rättslig grund tillämplig).

3.5 Samtycke

Personuppgifter får behandlas om den enskilde samtycker till att sådan behandling sker.

För att det ska vara lämpligt att stödja en behandling på samtycke så måste samtycket vara frivilligt. Med frivilligt menas att den registrerade har ett genuint fritt val och kontroll över sina personuppgifter. Den registrerade får exempelvis inte drabbas av negativa konsekvenser om den inte lämnar sitt samtycke.

För att samtycke ska kunna användas som rättslig grund måste maktförhållandet mellan den personuppgiftsansvarige och den registrerade också vara jämlikt. Tänk på att maktförhållandet ofta är ojämlikt i relationen mellan myndighet och medborgare, och mellan arbetsgivare och arbetstagare. Om det råder ett ojämlikt maktförhållande kan vi inte stödja oss på samtycke.

Datainspektionen ger följande exempel på situationer då en myndighet respektive arbetsgivare ändå kan använda sig av samtycke som rättslig grund:

Exempel 1: En kommunal nämnd planerar vägarbeten. Nämnden erbjuder invånarna möjlighet att anmäla sig för att få uppdateringar via e-post. Nämnden är tydlig med att det är frivilligt att anmäla sig och inhämtar samtycke för att använda e-

postadresserna för endast detta ändamål. Invånare som inte vill delta har inte gått miste om någon grundläggande service från myndigheten. Informationen finns även publikt på kommunens hemsida.

Exempel 2: En arbetsgivare vill filma på delar av kontoret. Arbetsgivaren frågar alla medarbetare som sitter på den berörda delen av kontoret efter deras samtycke, eftersom de kan synas i bakgrunden på filmen. De som inte vill bli filmade ska inte drabbas av några negativa konsekvenser, utan får istället likvärdiga arbetsplatser någon annanstans i byggnaden under den tid som filminspelningen pågår.

Att tänka på när samtycke används som rättslig grund är att den registrerade alltid har rätt att när som helst återkalla sitt samtycke. All behandling av den registrerades personuppgifter för det syfte som samtycket omfattat måste därmed upphöra. Återkallandet av samtycket påverkar dock inte lagligheten av den behandling av personuppgifterna som skett innan återkallelsen skedde.

På grund av ovanstående är det i många fall inte lämpligt eller kanske inte ens möjligt för oss att stödja oss på den registrerades samtycke som rättslig grund för en behandling. Överväg därför alltid först om ni kan stödja personuppgiftsbehandlingen på någon av de andra rättsliga grunderna.

Väljer man ändå att utföra en personuppgiftsbehandling som stödjer sig på samtycke som rättslig grund så ska man komma ihåg att det är personuppgiftsansvarig som ansvarar för att ett giltigt samtycke har inhämtas. Personuppgiftsansvarig behöver också kunna visa både att den registrerade har fått relevant information och att samtycket uppfyller uppställda krav. Följande måste därför alltid dokumenteras:

- Hur samtycket inhämtades.
- När samtycket inhämtades.
- Vilken information den registrerade fått.

3.6 Intresseavvägning

Den personuppgiftsansvarige får behandla personuppgifter utan den registrerades samtycke om den personuppgiftsansvariges intressen väger tyngre än den registrerades och om behandlingen är nödvändig för det aktuella ändamålet.

Observera att denna rättsliga grund enligt dataskyddsförordningen inte kan användas av myndigheter när de utför sina uppgifter.

4 De registrerades rättigheter

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

De registrerades rättigheter har utökats och förstärkts i dataskyddsförordningen jämfört med den tidigare gällande personuppgiftslagen.

4.1 Information innan personuppgifter börjar behandlas

Den registrerade har rätt att få information när personuppgifter om den registrerade behandlas. Det är den personuppgiftsansvarige (varje nämnd), som ska lämna informationen innan en behandling påbörjas.

I dataskyddsförordningen anges vilken information som ska ges. Informationen ska bland annat innehålla uppgifter om

- hur den enskilde kan komma i kontakt med den personuppgiftsansvarige,
- den rättsliga grunden för behandlingen och
- ändamålet med behandlingen.

Informationen ska anpassas till varje enskild personuppgiftsbehandling. Instruktioner om hur sådan information kan utformas finns i bilaga 2. I instruktionen finns även en översikt över vilken information som ska lämnas till den registrerade.

Om personuppgifterna hämtas från den registrerade själv, lämnas information lämpligast i samband med att uppgifterna samlas in.

Om personuppgifterna hämtas från någon annan part, ska den personuppgiftsansvarige istället lämna information i samband med att personuppgifterna första gången registreras.

Information behöver inte lämnas om det finns andra bestämmelser som gäller framför dataskyddsförordningen, till exempel om det finns uppgifter som omfattas av sekretess. Information behöver inte heller lämnas om sådant som den registrerade redan känner till, eller om det är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

4.2 Rätt till tillgång (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 staden särskilt framtagen e-tjänst för detta ändamål. E-tjänsten finns tillgänglig på stadens webbsida (https://helsingborg.se).

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. Det finns en instruktion för hantering av en sådan begäran, se bilaga 3.

Det skriftliga svaret ska inte innehålla sådana uppgifter som omfattas av sekretess mot den registrerade själv. Om registerutdrag begärs för ett barn av barnets vårdnadshavare ska utdraget inte heller innehålla uppgifter som omfattas av sekretess gentemot vårdnadshavaren.

4.3 Rätt till rättelse

Den registrerade har rätt att be att få felaktiga uppgifter rättade. Den enskilde har dessutom rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen.

Om en rättelse sker ska den personuppgiftsansvarige informera eventuella tredje parter som den personuppgiftsansvarige har lämnat uppgifter vidare till, att uppgifterna har rättats. Det gäller dock inte om det skulle visa sig omöjligt eller innebär en alltför betungande insats.

Det finns en instruktion för hantering av en begäran om rättelse, se bilaga 4.

4.4 Rätt till radering (”rätten att bli glömd”)

Den registrerade har rätt att begära att uppgifter som avser honom eller henne raderas.

Uppgifterna måste raderas utan dröjsmål i dessa fall:

- Om uppgifterna inte längre behövs för de ändamål som de samlades in för
- Om behandlingen grundar sig på den enskildes samtycke och denne återkallar samtycket
- Om behandlingen sker för direktmarknadsföring och den enskilde motsätter sig att uppgifterna behandlas
- Om den enskilde invänder mot personuppgiftsbehandling som sker för ett allmänt intresse eller efter en intresseavvägning (se avsnitt 3 ovan) och det inte finns berättigade skäl som väger tyngre än den enskildes intresse
- Om personuppgifterna har behandlats olagligt
- Om radering krävs för att uppfylla en rättslig skyldighet
- Om personuppgifterna avser barn och har samlats in i samband med att barnet skapar en profil i ett socialt nätverk

Om uppgifter raderas på den enskildes begäran ska nämnden – om det inte är omöjligt eller alltför betungande – informera dem som de har lämnat uppgifterna vidare till om raderingen. Observera att offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt inte ska betraktas som en sådan mottagare som behöver informeras om att radering skett.

Det finns undantag från rätten till radering om det är nödvändigt att behålla personuppgifterna för att tillgodose andra viktiga rättigheter som till exempel att uppfylla en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Av denna anledning bör det vara ovanligt att radering blir aktuell i offentlig verksamhet.

Det finns en instruktion för svar på en begäran om radering, se bilaga 4.

4.5 Rätt att invända mot och begära begränsning av en personuppgiftsbehandling

En enskild har i vissa fall rätt att invända mot den personuppgiftsansvariges behandling av dennes personuppgifter. Det gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning.

Den personuppgiftsansvarige får fortsätta behandla uppgifterna bara om det går att visa att det finns berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den enskildes intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och när denna har begärt att uppgifterna rättas. I sådana fall kan den registrerade även begära att behandlingen av uppgifterna begränsas under tiden som uppgifternas korrekthet utreds.

Det finns en instruktion för svar på en sådan förfrågan, se bilaga 4.

5 Ansvar och organisation

5.1 Personuppgiftsansvarig

I Helsingborgs stad är respektive nämnd och styrelse personuppgiftsansvarig, vilket framgår av respektive nämnds reglemente. Vidare är varje bolag och kommunalförbund personuppgiftsansvarig inom sitt verksamhetsområde.

Den personuppgiftsansvarige ansvarar enligt reglementena för att:

- föra register över de behandlingar av personuppgifter som sker i nämndens verksamhet,
- säkerställa laglig och korrekt behandling av personuppgifter,
- utse dataskyddsombud,
- delta i kommunens övergripande arbete med frågor om personuppgiftsbehandling och dataskydd; samt
- i övrigt fullgöra de uppgifter som ankommer på personuppgiftsansvarig enligt lag.

Kommunfullmäktige har uppdragit åt kommunstyrelsen att ha en samordnande roll i kommunens övergripande arbete med frågor om personuppgiftsbehandling och dataskydd. Stadsjuridiska enheten ansvarar för att fullgöra uppdraget.

5.2 Samordnare för dataskyddsfrågor

I varje nämnd eller styrelse ska det finnas en samordnare för dataskyddsfrågor som svarar för interna frågor om personuppgiftsbehandling. Även i stadens helägda bolag bör samordnare finnas. Samordnaren ska minst ansvara för följande uppgifter:

- föra förteckning över de personuppgiftsbehandlingar som sker i verksamheten,
- vara kontaktperson i dataskyddsfrågor för den egna förvaltningen och gentemot dataskyddsombudet samt
- ingå i ett stadsövergripande nätverk för dataskyddsfrågor.

Det är upp till varje nämnd att i övrigt utforma och planera hur arbetet kring dataskyddsfrågor ska genomföras.

5.3 Dataskyddsombud

Varje nämnd ska utse ett dataskyddsombud. Dataskyddsombudet ska självständigt övervaka och kontrollera att den personuppgiftsansvarige följer dataskyddsförordningen och angränsande regelverk och därtill ansvara för följande:

- att informera och ge råd till den personuppgiftsansvarige avseende regelverket,
- på begäran ge råd vad gäller konsekvensbedömningar avseende dataskydd,
- på begäran bistå i utredning av personuppgiftsincidenter,
- vara nämndens eller styrelsens kontakt mot enskilda och mot tillsynsmyndigheten,
- utöva tillsyn över den personuppgiftsbehandling som sker,

- genomföra utbildningar inom området,
- rapportera till organisationens ledning om dataskyddsfrågor och organisationens utvecklingsbehov minst en gång per år, samt ge förslag på åtgärder, samt
- på begäran bistå i andra frågor inom området.

Dataskyddsombudet utses genom beslut av nämnden. Datainspektionen ska informeras när ett nytt dataskyddsombud utses.

5.4 Nätverk för dataskyddsfrågor

Helsingborgs stad har ett nätverk för dataskyddsfrågor. Stadsjuridiska enheten är sammankallande samt ansvarar för att leda och driva stadsgemensamma frågor i nätverket. Nätverket består av representanter från stadens samtliga förvaltningar och helägda bolag samt medarbetare med kunskap inom IT och säkerhet.

6 Säkerhet vid behandling

Den personuppgiftsansvarige är skyldig att vidta lämpliga 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.

6.1 Inbyggt dataskydd (Privacy by design)

Inbyggt dataskydd (privacy by design) innebär att man tar hänsyn till integritetsskyddsreglerna 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.

6.2 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.

6.3 Konsekvensbedömning avseende dataskydd och förhandssamråd

Den personuppgiftsansvarige måste i vissa fall göra en konsekvensbedömning avseende dataskydd vid behandling av personuppgifter som innebär förhöjda integritetsrisker.

Den personuppgiftsansvarige ska rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd.

Om konsekvensbedömningen avseende dataskydd visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken måste den personuppgiftsansvarige också samråda med Datainspektionen (så kallat förhandssamråd) innan behandlingen påbörjas.

Datainspektionen kan i förhandssamrådet utfärda råd, förelägganden eller förbud som säkerställer att behandlingen är i enlighet med förordningens regler.

Instruktion för genomförande av en konsekvensbedömning avseende dataskydd inklusive mall för bedömningen finns i bilaga 5.

6.4 Åtgärder vid personuppgiftsincident

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.

Helsingborgs stad har en e-tjänst för rapportering av misstänkta eller inträffade personuppgiftsincidenter.

Respektive nämnd 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 Datainspektionen 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.

Utgångspunkten är att alla personuppgiftsincidenter ska rapporteras internt, även de som eventuellt ska anmälas till Datainspektionen.

Instruktion för att hantera och dokumentera en personuppgiftsincident finns i bilaga 6.

7 Övrigt

7.1 Personuppgifter i allmänna handlingar

Helsingborgs stad behandlar en stor mängd personuppgifter i handlingar som finns hos oss. Det ligger på respektive nämnd att hantera brev eller e-post som innehåller personuppgifter på ett säkert sätt, så som i säkra verksamhetssystem.

7.2 Känsliga personuppgifter i e-post

Känsliga personuppgifter ska som huvudregel inte skickas via e-post. Vid kontakt med andra myndigheter ska, i de fall myndigheten har det, funktioner för säkra meddelanden tillämpas.

Om vi får in känsliga uppgifter via e-post bör de tas bort från e-postsystemet så snart som möjligt. Om vi har rättslig grund för att spara uppgifterna så bör de så snart som möjligt överföras till det system där de hör hemma – till exempel ett ärendehanteringssystem eller en gemensam mapp (G:).

E-post som kommer in till Helsingborgs stad blir normalt en allmän handling som ska registreras eller hållas ordnad. Vi är enligt arkivlagen skyldiga att bevara allmänna handlingar. Utgångspunkten är att det är tillåtet att behandla personuppgifter för att uppfylla kraven i arkivlagen om bevarande av allmänna handlingar.

7.3 Publicering av personuppgifter i webbdiariet

Helsingborgs stad publicerar allmänna handlingar i sitt webbdiarium (http://diariet.helsingborg.se).

Utgångpunkten är att handlingar som är offentliga i sin helhet ska publiceras.

Enskilda handlingar som innehåller personuppgifter som är känsliga, skyddsvärda eller omfattas av sekretess enligt offentlighets- och sekretesslagen, ska inte publiceras. Om det finns sådana uppgifter i en handling, ska handlingen inte publiceras alternativt ska uppgifterna tas bort (”maskas”) innan publicering sker.

8 Rättsliga konsekvenser

Ansvaret för behandling av personuppgifter, som ytterst ligger på varje nämnd, är skadeståndssanktionerat.

Varje person som lidit materiell eller immateriell skada till följd av överträdelser av EU:s dataskyddsförordning har rätt till ersättning av personuppgiftsansvarige för den uppkomna skadan (skadestånd).

Dessutom kan Datainspektionen i vissa fall döma ut en administrativ sanktionsavgift när en organisation missköter sin behandling av personuppgifter. Sanktionsavgiften för myndigheter kan som mest uppgå till 10 miljoner kronor per överträdelse.

Datainspektionen kan även utfärda varningar om en planerad behandling av personuppgifter sannolikt kommer att bryta mot bestämmelserna i EU:s dataskyddsförordning. Datainspektionen kan utfärda reprimander om en pågående behandling av personuppgifter bryter mot bestämmelserna och kan dessutom förelägga en personuppgiftsansvarig till exempel att de måste upphöra med en viss behandling.