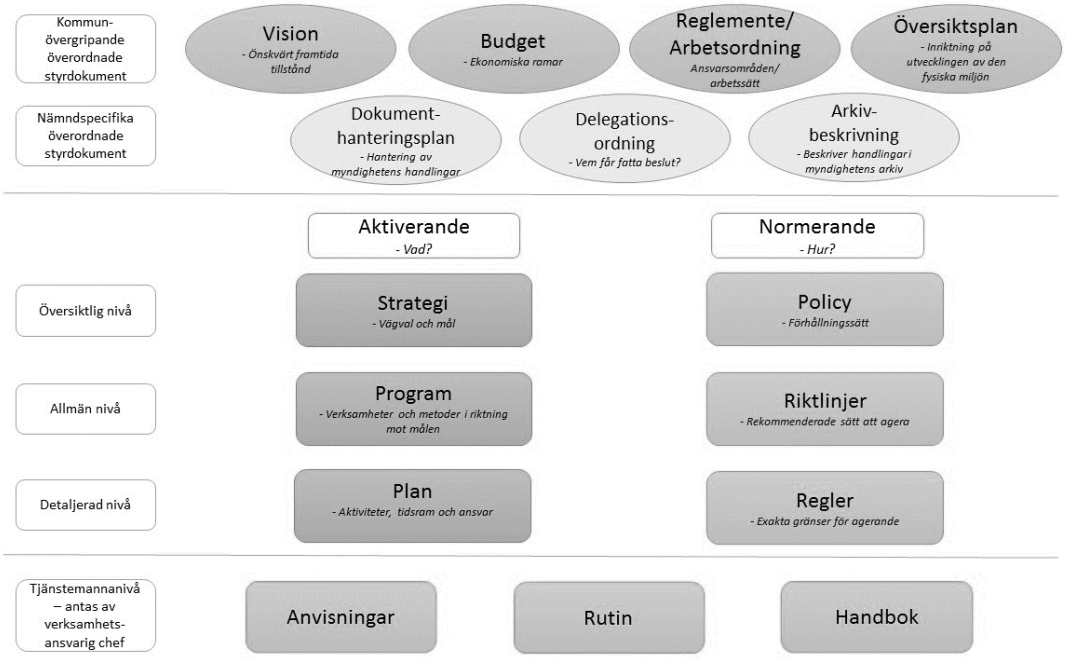
RIKTLINJER FÖR

Hantering av person-uppgifter

HÅBO KOMMUN

Antaget av	Kommunfullmäktige
Antaget	2018-05-07 § 51
Giltighetstid	Tillsvidare
Dokumentansvarig	Dataskyddsombudet

Håbo kommuns styrdokumentshierarki



Diarienummer	KS 2018/00126 nr 81030
Gäller för	Samtliga nämnder och bolag
Tidpunkt för aktualitetsprövning	2022-12-31

Riktlinjer för hantering av personuppgifter

Innehåll

Håbo kommuns styrdokumentshierarki 2

1. Inledning 4

2. Syfte 4

3. Avgränsning 4

4. Definitioner 4

5. Behandling av personuppgifter 7

Laglig grund, Artikel 6 7

Laglig grund, Artikel 9 2 9

6. Säkerhet 11

7. Registerförteckning 12

8. Informationsplikt 13

9. Externt företags hantering av personuppgifter för kommunens räkning 14

10. Publicering av personuppgifter på Internet 14

11. Gallra personuppgifter 15

12. Registerutdrag och dataportabilitet 16

1. Inledning
Den 25 maj 2018 träder den europeiska Dataskyddsförordningen i kraft. Dataskyddsförordningen är en modernisering av tidigare Personuppgiftslagstiftning och ställer mer långtgående krav på Håbo kommuns behandling av personuppgifter.

2. Syfte
Dessa riktlinjer har som syfte att utgöra ett kommunövergripande ramverk för personuppgiftshantering i Håbo kommun samt att tydligt definiera den kommunala organisationen kring arbetet med personuppgifter. Riktlinjerna gäller för samtliga nämnder och bolag i kommunen.

3. Avgränsning
Riktlinjerna utgör inte ett detaljerat ramverk för kommunens informationssäkerhetsarbete, IT-verksamhet eller kommunikationsstrategiska arbete. Det hanteras istället i kommunens styrdokument för IT och kommunikation.

4. Definitioner

4.1 Personuppgift
Information som direkt eller indirekt kan knytas till en (fysisk) person som är i livet är en personuppgift. Uppgiften kan enskilt eller i kombination med andra upplysningar knytas till en levande person om man av den registrerade uppgiften kan förstå vem det handlar om.

Exempel på direkta personuppgifter är namn, personnummer, födelsedatum och fotografier medan IP-adress, fastighetsbeteckning, kontonummer och användar-ID är exempel på indirekta personuppgifter. Även initialer och annan typ av krypterad eller kodad information kan vara en personuppgift om det med hjälp av anslutande uppgifter går att förstå vem det rör sig om.

4.2 Behandling av personuppgift
I Dataskyddsförordningen talar man om behandling av personuppgifter. Med behandling menar man allt som görs med personuppgifterna. Det kan exempelvis röra sig om insamling av personuppgifter, likaså registrering, lagring och spridning. Lagringen kan ske till exempel lokalt på en dator, på en samarbetsyta eller en server.

Här följer några exempel på vanliga behandlingar av personuppgifter:

- Kund- och leverantörsregister (kontaktpersoner och enskilda näringsidkare).
- Elektroniska besöksliggare och passersystem.
- Filmer, bilder och foton av alla slag, på anställda såväl som enskild privatperson.
- Ekonomisystem, ärendehanteringssystem och övriga verksamhetssystem.
- Pensionslistor.
- Medarbetarsamtal, lönesamtal och utvärderingar av verksamheten (på individnivå).
- Kontaktinformation till kolleger så som intern telefonkatalog och kontakter i epostsystemet.
- Behörighetsadministration och behandlingshistorik (loggar).
- GIS-system (Geografiska Informationssystem).
- Kameraövervakning eller bevakning.

- Spontanansökningar, rekryteringsdatabaser, kompetensdatabaser, personlighetstester/profiler.
- Intranät och publik webbplats.
- Egen registerförteckning - till exempel systemägare och kontaktperson för registerutdrag.
- Kontaktcentrets IT-system (lagrar ofta information om vem, anknytning som har ringt till vem och när).
- System som inte längre används.

4.3 Känsliga personuppgifter

I Dataskyddsförordningen (Artikel 9) finns ett generellt förbud mot att registrera känsliga personuppgifter. Bestämmelsen betyder inte att det är helt förbjudet att registrera känsliga personuppgifter, men utgångspunkten är att det är förbjudet och man behöver därför ha stöd av undantagen (Artikel 9 2 a-j) i förordningen för att det ska vara tillåtet.

Känsliga uppgifter definieras som:

- Ras eller etniskt ursprung (exempelvis uppgifter om modersmål, födelseland eller tolkbehov).
- Politiska åsikter (exempelvis medlemskap i politiskt parti).
- Religiös eller filosofisk övertygelse (exempelvis medlem i religiöst samfund, särskilda önskemål om mat eller andra behov som har religiös koppling).
- Medlemskap i fackförening.
- Hälsoinformation (exempelvis sjukfrånvaro, behov av hjälpmedel pga. funktionsnedsättning eller placering i särskoleklass).
- Sexualliv (inklusive uppgifter om sexuell läggning).
- Genetiska uppgifter (uppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken, som kan framgå genom exempelvis DNA-analys).
- Biometriska uppgifter (uppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken som erhållits genom en särskild teknisk behandling, exempelvis fingeravtryck).

4.4 Integritetskänsliga personuppgifter

Datainspektionen har gjort en skillnad mellan känsliga personuppgifter (ovan stycke) och andra personuppgifter som man anser vara extra skyddsvärda eller integritetskänsliga men som inte omfattas av definitionen om känsliga personuppgifter.

Exempel på sådana uppgifter är:

- Personuppgifter som omfattas av sekretess eller tystnadsplikt (eller annan särlagstiftning, exempelvis Patientdatalagen).
- Personnummer.
- Uppgifter om personliga och ekonomiska förhållanden.
- Bild-, ljud- och videoinspelningar.
- Omdömen och personlighetsbeskrivningar (preferenser, pålitlighet, beteenden mm.).
- Uppgifter om barn.
- Uppgifter om lagöverträdelser.

Datainspektionen har ställt krav på att starka säkerhetsåtgärder vidtas för det fall sådana integritetskänsliga personuppgifter på något sätt registreras så att de finns att nå via Internet (öppna nät), exempelvis efter inloggning.

4.5 Personuppgiftsansvarig
Varje nämnd och kommunalt bolag i Håbo kommun är personuppgiftsansvarig för de behandlingar av personuppgifter som görs inom nämnden eller bolagets verksamhet. Personuppgiftsansvarig är alltid en juridisk person, det går alltså inte att delegera personuppgiftsansvaret till en fysisk person. Ansvaret gentemot tillsynsmyndigheten och de registrerade ligger alltid kvar på den personuppgiftsansvarige till exempel när det gäller skadeståndsanspråk.

Det är personuppgiftsansvariges skyldighet att vidta tekniska och organisatoriska åtgärder för att säkerställa att all behandling av personuppgifter följer Dataskyddsförordningen och där till kommande lagstiftning.

4.6 Personuppgiftsbiträde
Personuppgiftsbiträde är den som behandlar personuppgifter för en personansvariges räkning. Ett personuppgiftsbiträde finns alltid *utanför* den personuppgiftsansvariges organisation. En typisk biträdessituation är till exempel när en IT-leverantör processar information i sina datorer för den personuppgiftsansvariges räkning genom att exempelvis trycka fakturor eller adresser. Det kan också vara företag som sköter passersystem eller en webbtjänst.

En biträdessituation behöver inte endast handla om lagring av personuppgifter, utan gäller även när en extern part har åtkomst till personuppgiftsansvariges data genom sitt uppdrag för service, support, underhåll, utveckling och liknande. Dataskyddsförordningen kräver att ett personuppgiftsbiträdesavtal upprättas mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

I Dataskyddsförordningen blir även personuppgiftsbiträdet skyldigt att föra en förteckning över sina personuppgiftsbehandlingar och vidta lämpliga säkerhetsåtgärder.

Personuppgiftsbiträdet kan även komma att bli föremål för tillsyn, administrativa sanktionsavgifter samt bli skadeståndsskyldig.

4.7 Dataskyddsombud
Ett dataskyddsombud är en person som ser till att personuppgifter behandlas på ett korrekt och lagligt sätt inom den egna organisationen samt är kontaktperson för tillsynsmyndigheter och allmänhet. Dataskyddsombudet kan jämföras med en internrevisor som påpekar fel och brister till den som är personuppgiftsansvarig.

När den personuppgiftsansvarige (nämnden eller bolaget) utsett ett dataskyddsombud anmäls det till Datainspektionen.

4.8 Helt eller delvis automatiserad behandling
Dataskyddsförordningen tillämpas på all behandling av personuppgifter som utförs helt eller delvis med hjälp av datorer. Att lagen även omfattar delvis automatiserad behandling innebär bland annat att den gäller redan när någon samlar in personuppgifter manuellt, exempelvis genom en pappersenkät, med syfte att senare registrera uppgifterna digitalt.

Det innebär också att till exempel muntligt utlämnande eller utlämnande på papper av personuppgifter som lagras digitalt omfattas av lagen.

4.9 Manuella register
Manuell behandling av personuppgifter i register (till exempel ett klassiskt kartotek eller närarkiv) omfattas av Dataskyddsförordningen om uppgifterna är sorterade enligt något slags system som gör det möjligt att söka bland uppgifterna.

En hög med papper på ett skrivbord anses inte vara ett register även om de är sorterade i bokstavsordning efter efternamn. För att det ska vara ett manuellt register som omfattas av Dataskyddsförordningen krävs att samlingen av personuppgifter är strukturerad i syfte att påtagligt underlätta eftersökning och sammanställning av personuppgifter.

5. Behandling av personuppgifter

5.1 Behandlingen ska vara nödvändig
För all behandling av personuppgifter i Håbo kommun finns alltid ett krav på nödvändighet. Nödvändighet ska i sammanhanget förstås som att behandlingen innebär betydande effektiviseringsvinster för kommunen, dvs att utan personuppgiftsbehandlingen så skulle det förfarande som behandlingen grundar sig på bli väsentligt mer tidskrävande och kostnadsdrivande för kommunen. Nödvändighetskravet innebär också att alla personuppgifter som samlas in ska vara nödvändiga för ändamålet för vilka de samlas in, och att inga onödiga eller extra personuppgifter ska samlas in. Samtliga nämnder och kommunala bolag i Håbo kommun ansvarar för att, inom egen verksamhet, överväga om nödvändighetskravet är uppfyllt inför varje behandling av personuppgifter.

5.2 Laglig grund - personuppgifter
För att Håbo kommun ska kunna behandla personuppgifter krävs, förutom uppfyllandet av nödvändighetskravet ovan, att behandlingen har stöd i en laglig grund. De lagliga grunderna för personuppgiftsbehandling återfinns i Artikel 6 a-f i Dataskyddsförordningen och innebär i huvudsak följande:

Laglig grund, Artikel 6
Samtycke a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
Avtal 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.
Rättslig förpliktelse c) Behandlingen är nödvändig för att fullgöra en laglig förpliktelse som åvilar den personuppgiftsansvarige.

Skydd för grundläggande intressen d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
Uppgift av allmänt intresse och myndighetsutövning e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
Efter en intresseavvägning f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigande 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.

Respektive personuppgiftsansvarige i Håbo kommun ansvarar för att den personuppgiftsbehandling som sker inom den personuppgiftsansvariges verksamhetsområde har stöd i *åtminstone* en av ovanstående lagliga grunder.

5.2.1 Särskilt om samtycke

Brukandet av samtycket som rättlig grund för personuppgiftsbehandling i kommunal verksamhet har försvagats i Dataskyddsförordningen i jämförelse med tidigare personuppgiftslagstiftning. Bland annat innebär det att kommunens verksamheter inte kommer att använda samtycke som stöd för den personuppgiftsbehandling som sker som del av myndighetsutövning eller i de fall det annars råder en påtaglig skillnad i makt mellan den som är eller blir registrerad och den personuppgiftsansvarige, exempelvis vid ingången av ett anställningsavtal eller i andra likande fall där den registrerade inte har några realistiska alternativ annat än att acceptera att dennes personuppgifter samlas in och behandlas.

Ett nekande till samtycke får inte heller innebära att den registrerade på andra sätt inte kan eller får tal del av en grundläggande kommunal service.

Exempel där samtycke skulle kunna användas är:

- Vid publicering av foto, filmer eller likande på webbplats eller motsvarande.
- Vid insamling av kontaktuppgifter till en e-postlista, under förutsättning att informationen går att ta del av, och är tillgänglig, på annat sätt.

I övrigt så måste ett samtycke alltid kunna återtas av den registrerade. Ett sådant återtagande innebär att den personuppgiftsansvarige ska upphöra med den personuppgiftsbehandling som samtycket grundade sig på, och sedan gallra eller anonymisera personuppgifterna.

Den personuppgiftsansvarige ansvarar för att kunna påvisa ett givet samtycke som grund för en specifik behandling. Detta görs enklast genom användning av samtyckesmallar som tillhandahålls av dataskyddsombudet. I de fall där samtycket ges som del i en e-tjänst, eller motsvarande, ansvarar den personuppgiftsansvarige för att se till att samtycket sparas på ett tillfredställande sätt och att informationen om samtycket uppfyller de krav som Dataskyddsförordningen ställer.

Sammanfattningsvis så ska samtycke som laglig grund användas sparsamt av de kommunala verksamheterna, och dessa ska om oklarheter om samtyckets riktighet uppstår alltid rådgöra med dataskyddsombudet.

5.3 Laglig grund – känsliga personuppgifter
De lagliga grunderna för behandling av känsliga personuppgifter återfinns i Artikel 9 2 a-j i Dataskyddsförordningen och innebär i huvudsak följande:

Laglig grund, Artikel 9 2
Samtycke a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål, utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet i punkt 1 inte kan upphävas av den registrerade.
Skyldighet inom arbetsrätt b) Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.
Social trygghet/skydd c) Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
Vitalt intresse d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.
Uppgift offentliggjord e) Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
Rättsligt anspråk f) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.

Hälso- och sjukvård g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
Arkivändamål h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.
Viktigt allmänt intresse/Myndighetsbehandling i vissa fall i) Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten eller medlemsstaternas nationella rätt, där lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt.
j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

5.4 Personuppgifter i e-post

E-post som innehåller personuppgifter kan skickas så länge de inte innehåller:

- Känsliga/integritetskänsliga personuppgifter
- Sekretessuppgifter enligt Offentlighets- och sekretesslagen.

I vissa fall behöver kommunens verksamheter skicka e-post som innehåller känsliga personuppgifter/sekretess i sin helhet och då krävs att särskilda säkerhetsåtgärder vidtas. Med säkerhetsåtgärder innebär i praktiken krypteringsskydd på ett sådant sätt att endast den avsedda mottagaren kan ta del av uppgifterna.

Om någon skickar känsliga personuppgifter eller sekretessuppgifter till kommunen så innebär det inte att denne har gett samtycke till att hantera dessa personuppgifter per e-post. Därför ska dessa uppgifter tas bort i svar eller vidarebefordran av den ursprungliga e-posten.

5.5 Personnummer
Även om ett personnummer inte är en känslig personuppgift så betraktas den som extra skyddsvärd och får därför inte används hur som helst. Personnummer får endast samlas in och behandlas om:

- Om behandlingen är klart motiverad med hänsyn till ändamålet med behandlingen.
- Om behandlingen är klart motiverad med hänsyn till vikten av en säker identifiering, (exempelvis i ett löneadministrativt IT-system, redovisning av källskatter, vid rehabiliteringsutredning eller kommunikation med facket i lönerevisioner, kommuninvånarregister, i ett skoladministrativt IT-system).
- Om behandlingen är klart motiverat med hänsyn till något annat beaktansvärt skäl.

Kommunens personuppgiftsansvariga ska särskilt beakta och aktivt motverka en slentrianmässig användning av personnummer.

Personnummer ska som huvudregel inte användas som användaridentitet vid inloggning i olika typer av verksamhetssystem. Om det finns behov av att använda personnummer som inloggning så ska den personuppgiftsansvarige samråda med dataskyddsombudet.

6. Säkerhet
Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna. Till tekniska åtgärder räknas saker som brandväggar, krypteringsfunktioner och antivirus, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation, styrdokument och dokumenterade rutiner. Behandling av integritetskänsliga personuppgifter ställer högre krav på säkerhetsåtgärder.

Följande frågeställningar kan vara till hjälp när man bedömer hur pass integritetskänsliga uppgifterna är:

- Omfattas uppgifterna av tystnadsplikt eller sekretess enligt Offentlighets- och sekretesslagen (2009:400) eller annan lagstiftning?
- Omfattas behandlingen av någon särlagstiftning, till exempel Patientdatalagen (2008:355) eller
  Lagen om behandling av personuppgifter inom socialtjänsten (2003:763) med flera?
- Är det uppgifter om lagöverträdelser?
- Är det uppgifter om enskildas personliga förhållanden?

Om svaret på någon av dessa frågor är JA så ska säkerhetsåtgärderna för att skydda personuppgifterna vara mer omfattande.

Lämplig säkerhetsnivå för olika grader av informationskänslighet fastställs i kommunens styrdokument för IT.

6.1 Särskilda risker och lämpliga säkerhetsåtgärder
Utöver att bedöma graden av känslighet ska varje personuppgiftsansvarig ta ställning till vilka särskilda risker det finns med behandlingen av personuppgifterna. I det arbetet kan följande frågeställningar vara vägledande:

- Behandlas personuppgifterna på ett sätt som gör det svårt att kontrollera att det bara sker i enlighet med ändamålen med behandlingen?
- Finns det risk för att personuppgifterna kan spridas på ett oönskat sätt både externt och internt?
- Hanteras personuppgifter via öppna nät som Internet, till exempel via en webbsida eller genom e-post?
- Kan många användare komma åt personuppgifterna?
- Behandlas personuppgifter om många personer?
- Behandlas en stor mängd personuppgifter om varje person?

Ju mer svaret på frågorna är JA, desto mer omfattande bör säkerhetsåtgärderna vara.

Den faktiska hanteringen av kommunens informationssäkerhetsklassning hanteras i kommunens styrdokument för IT.

Personuppgiftsansvarig ansvarar för att årligen i sin interna kontroll pröva om införda säkerhetsåtgärder tillhandahåller ett tillräckligt gott skydd. T.ex. via systematisk genomgång av systemloggar osv.

6.2 Konsekvensbedömning
Enligt Dataskyddsförordningen så har den personuppgiftsansvarige en skyldighet att genomföra en så kallad konsekvensbedömning, en typ av risk- och sårbarhetsanalys, för varje *ny* behandling av känsliga personuppgifter. Med hjälp av frågeställningar om säkerhetsåtgärder och risker är konsekvensbedömningen ett effektivt hjälpmedel för den personuppgiftsansvarige att säkerställa en korrekt behandling av personuppgifter.

Kravet på konsekvensbedömningar gäller endast verksamhetssystem som tas i bruk fr.o.m. den 25 maj 2018.

Dataskyddsombudet tillhandahåller en mall för konsekvensbedömning och bistår med stöd i genomförandet av dessa.

6.3 Incidentrapportering
Om det inträffar en säkerhetsincident som rör personuppgifter, till exempel ett dataintrång eller en oavsiktlig förlust av personuppgifter, så är kommunens personuppgiftsansvariga enligt Dataskyddsförordningen skyldiga att dels dokumentera och rapportera incidenten till Datainspektionen inom 72 timmar och dels informera de registrerade till exempel om det finns risk för identitetsstöld eller bedrägeri.

Rutin för hantering av personuppgiftsincidenter tillhandahålls, underhålls och utvecklas av dataskyddsombudet.

7. Registerförteckning
Kommunens personuppgiftsansvariga är enligt Dataskyddsförordningen skyldiga att föra register över sina behandlingar av personuppgifter. Innehållet i registerförteckningarna framgår uttryckligen av Dataskyddsförordningen Artikel 30 och ska till exempel innehålla:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.

- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inklusive mottagare i tredjeländer eller i internationella organisationer.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation,.De förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- En allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna omkring behandlingen.

Kommunens personuppgiftsansvariga ansvarar för att dess registerförteckningar uppdateras löpande och att eventuella tillkommande behandlingar anmäls till dataskyddsombudet.

Registermall tillhandahålls och uppdateras av dataskyddsombudet. Respektive personuppgiftsansvarig ansvarar för att hanteringen av personuppgiftsansvariges register underhålls.

8. Informationsplikt

Enligt Dataskyddsförordningen har den personuppgiftsansvarige en långtgående informationsplikt gentemot de registrerade, både när uppgifter samlas in av den personuppgiftsansvarige och när den personuppgiftsansvarige samlar in uppgifterna från någon annan (t.ex. myndighet eller kommun). Information måste även lämnas vid händelse av dataintrång och det finns risk för exempelvis bedrägeri eller identitetsstöld (incidentrapportering).

Informationen ska bland annat innehålla:

- Kontaktuppgifter till den personuppgiftsansvarige.
- Den lagliga grunden för behandlingen.
- Ändamålet med behandlingen.
- Information om personuppgifterna kan komma att lämnas ut till tredje part och i så fall för vilka syften.
- Rätten att begära registerutdrag.
- Rätten att få sina personuppgifter rättade vid felaktigheter eller raderade.
- Hur länge personuppgifterna kommer att lagras.

Om redan insamlade personuppgifter kommer att användas för ett annat syfte (ändamål) än för vilket de samlades in måste ny information lämnas till de registrerade – det vill säga information om ändamålet för den nya behandlingen.

Informationen ska lämnas till den registrerade kostnadsfritt i en lättillgänglig, skriftlig form (vilket kan vara i elektronisk form) och med ett tydligt och enkelt språk.

Dataskyddsombudet tillhandahåller, underhåller och uppdaterar övergripande informationstexter som ska används av samtliga personuppgiftsansvariga i Håbo kommun. Det är den personuppgiftsansvariga som ansvarar för att informationen är korrekt i förhållande till de enskilda behandlingarna inom dess verksamhetsområde.

9. Externt företags hantering av personuppgifter för kommunens räkning

När externa parter, som till exempel en systemleverantör eller support, behandlar personuppgifter åt kommunens personuppgiftsansvariga kallas den externa parten för *personuppgiftsbiträde*.

Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Personuppgiftsbiträdet behöver inte lagra personuppgifterna utan det räcker att den externa parten har tillgång till den personuppgiftsansvariges data för att räknas som ett personuppgiftsbiträde.

9.1 Personuppgiftsbiträdesavtal

Enligt Dataskyddsförordningen ska det i alla biträdessituationer finnas ett skriftligt avtal mellan den personuppgiftsansvarige och biträdet. I ett sådant avtal villkoras biträdets hantering av personuppgifterna samt om biträdet i sin tur får ge andra externa parter (s.k. underbiträden) tillgång till uppgifterna. I Håbo kommun ska biträdesavtalet vara en del av tjänsteavtalet, och därmed beaktas från början, i upphandlingsprocessen.

Mallar för personuppgiftsbiträdesavtal underhålls, uppdateras och tillhandahålls av dataskyddsombudet.

Det är dock den personuppgiftsansvarige som ansvarar för att erforderliga avtal ingås.

10. Publicering av personuppgifter på Internet

Personuppgifter om enskilda, till exempel namn, får publiceras på hemsidan om publiceringen har stöd i någon av de lagliga grunderna för personuppgiftsbehandling och om dessa och övriga publicerade uppgifter, enskilt eller sammantaget, inte kan antas leda till att den registrerades personliga integritet kränks.

Det innebär att personuppgifter inte får publiceras i kombination med information som innehåller integritetskänslig information, rör lagöverträdelser eller omfattas av sekretess/tystnadsplikt.

Publicering av uppgifter på Internet ska inte förväxlas med Offentlighetsprincipen. Enbart det faktum att en handling är allmän och offentlig innebär inte att det är tillåtet att publicera den på hemsidan. Enligt Offentlighetsprincipen finns det heller ingen *skyldighet* att publicera information på Internet. Det innebär i sin tur att Dataskyddsförordningens regler måste följas när det kommer till webbpublicering.

Ex. en nämnd beslutar om att vitesförelägga en privatperson för brott mot miljöbalken.

Beslutet hanteras enligt:

Offentlighetsprincipen
Om någon begär att få ta del av beslutet så är det en offentlig handling och ska lämnas ut skyndsamt.

Dataskyddsförordningen
Eftersom handlingen innehåller känslig information om lagöverträdelser ska handlingen inte publiceras på hemsidan.

10.1 Webbdiarium och anslagstavla
För protokoll, kallelser och eventuella handlingar som publiceras på kommunens digitala anslagstavla och webbdiarier gäller Dataskyddsförordningen. Personuppgifter som direkt pekar ut en enskild får inte publiceras på hemsidan, undantaget förtroendevalda i deras roll som förtroendevalda och tjänstemän i deras roll som tjänstemän.

Direkt utpekande uppgifter är exempelvis namn och personnummer, indirekta uppgifter är exempelvis fastighetsbeteckning. Det är dock de enskilda uppgifterna i handlingarna som ska döljas, inte hela dokumentet.

10.2 Publicering och spridning av foto och film
Att publicera foton kräver i regel samtycke. Det finns dock undantag där det allmänna intresset gör det tillåtet att publicera foton, exempelvis foton av förtroendevalda och nyckelfunktioner inom kommunen i kombination med namn och eventuella kontaktuppgifter.

Inom skola, förskola och fritids måste båda vårdnadshavarna samtycka innan publicering om det gäller barn under 13 år. Från 13 år och uppåt kan barnet själv ge sitt samtycke.

När Håbo kommun som organisation publicerar personuppgifter, med stöd av någon av de lagliga grunderna, i sociala medier (Facebook, Twitter, Instagram, Youtube m.fl.) så finns ett personuppgiftsansvar.

I personuppgiftsansvaret ingår att:

- Inte publicera kränkande personuppgifter.
- Hålla regelbunden uppsikt över publiceringarna för att upptäcka kränkande personuppgifter.
- Skyndsamt ta bort kränkande personuppgifter.
- Vidta lämpliga säkerhetsåtgärder (utbildning och instruktioner till de som arbetar med sociala medier för organisationens räkning, anställda och andra som agerar på uppdrag av kommunen).
- Tillse att det hålls en god ton bland besökarna på till exempel kommunens Facebook-sida.

Detta regleras i detalj i kommunikationsenhetens styrdokument.

11. Gallra personuppgifter
Det är ändamålet, alltså anledningen till varför personuppgifter samlas in och behandlas som avgör hur länge de får bevaras. Grundregeln är att personuppgifter inte ska bevaras längre än vad som är nödvändigt. En nämnd eller ett bolag har dock skyldighet att tillse att allmänna handlingar arkiveras, bevaras och tas om hand av kommunens arkivmyndighet. I dessa fall har bestämmelserna i Arkivlagen, Tryckfrihetsförordningen, Offentlighets- och sekretesslagstiftningen samt eventuella registerlagar företräde framför Dataskyddsförordningen.

Arkivering innebär att handlingen tas bort från till exempel ett administrativt register som används i den dagliga verksamheten. Arkivet kan finnas tillgängligt i samma datasystem, men måste då innehålla tekniska avgränsningar. Behörighet till den arkiverade

informationen ska ges till de personer som behöver information för att kunna utföra sitt arbete.

11.1 Gallring av personuppgifter
Det finns två olika sätt att ta bort personuppgifter. Man kan antingen avidentifiera eller förstöra (gallra) dem:

Avidentifiera

Att avidentifiera personuppgifterna innebär att man avlägsnar alla identifieringsmöjligheter så att de uppgifter som fortsättningsvis behandlas inte längre går att koppla samman med en fysisk person. Krypterade personuppgifter är inte avidentifierade så länge någon kan göra uppgifterna läsbara och därmed identifiera personen.

Förstöra (gallra)

Att förstöra personuppgifterna innebär att se till att de inte går att återskapa.. Hur långtgående tekniska åtgärder som bör vidtas är bland annat beroende av informationens känslighet.

11.2 Dokumenthanteringsplan
Gallring inom kommunens verksamheter får inte ske utan att gallringen medges i, av den personuppgiftsansvarige, antagen dokumenthanteringsplan. Dokumenthanteringsplanen gäller både för digitala handlingar och fysiska handlingar. Av dokumenthanteringsplanen framgår även om speciallagstiftning anger särskild gallringsfrist (till exempel Patientdatalagen).

Varje personuppgiftsansvarig ansvarar för att dokumenthanteringsplanen revideras vid behov, dock minst en gång om året, och för att systematisk gallring av personuppgifter genomförs.

12. Registerutdrag och dataportabilitet
Alla har rätt att vända sig till kommunen och begära att få veta vad som finns registrerat om dem. Ett registerutdrag innebär att den personuppgiftsansvarige ska lämna information om vad som finns registrerat om en specifik person. Utdraget får bara gälla den person som har begärt det, självklart kan ingen begära ett registerutdrag gällande någon annan person (det finns vissa undantag avseende förvaltare, gode män och vårdnadshavare).

I vissa fall äger de registrerade rätten att få ut sina personuppgifter i ett maskinläsbart format för att t.ex. vidareutnyttja dem någon annanstans.

Rutin för hur denna rättighet hanteras i Håbo kommun utvecklas och underhålls av dataskyddsombudet.