Huddinge

RIKTLINJE

Beslutad av	Dokumentansvarig	Gäller fr o m	Senast reviderad	Diarienummer	Typ av styrdokument
Namn	Säkerhetschefen	2019-LL-LL	Klicka för att ange datum	KS-2019/336.112	Normerande

Riktlinjer för behandling av personuppgifter (HKF 1500)

1. Bakgrund

Dataskyddsförordningen, även benämnd GDPR, innehåller regler för hur man får behandla personuppgifter inom EU. Förordningen började gälla den 25 maj 2018 och ersatte då personuppgiftslagen (PuL). Syftet med lagstiftningen är att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas. Dataskyddsförordningen tillsammans med dataskyddslagen som också trädde i kraft den 25 maj 2018 utgör regelverket för behandling av personuppgifter i Sverige.

Det bör noteras att annan speciallagstiftning kan vara tillämplig beroende på vilken förvaltning inom kommunen som hanterar personuppgifter. Exempel på en sådan lagstiftningen är Brottsdatalagen (2018:1177) samt Lagen (2001:454) om behandling av personuppgifter inom socialtjänsten (SoLPuL). Dessa riktlinjer kommer inte behandla sådan speciallagstiftning men de bör uppmärksammas och följas av respektive förvaltning.

Enligt Artikel 32 i dataskyddsförordningen ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska säkerhetsåtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Huddinge kommun har därför valt att ta fram dessa riktlinjer för behandling av personuppgifter.

Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska och organisatoriska åtgärder. Kommunen ska ansvara för och kunna visa att detta efterlevs såväl som förmågan att återställa tillgängligheten och tillgången vid en incident samt ett förfarande för att regelbundet testa, undersöka och utvärdera åtgärdernas lämpliga säkerhetsnivå.

Huddinge kommun har tagit fram riktlinjer inom olika områden för att underlätta och säkerställa integritetsskyddsarbetet inom kommunen. Nedan följer en generell information om de krav som ställs på den personuppgiftsansvarige tillsammans med de specifika riktlinjer som kommunen tagit fram inom respektive område. Kommunstyrelsen har genom sin förvaltning en stödjande och samordnade roll gentemot övriga förvaltningar för att underlätta arbetet.

2. Syfte och mål

Syftet med riktlinjerna är att ge kommunens verksamheter ett stöd för hur arbetet med personuppgiftsbehandlingar ska utföras och bedrivas effektivt, med god kvalitet och enligt tillämpliga lagstiftningar.

Målet är att Huddinge kommun ska beakta och upprätthålla de registrerades integritet och rättigheter i allt arbete som bedrivs i kommunens verksamheter.

3. Vad är en personuppgift?

Personuppgift är information som direkt eller indirekt kan knytas till en (fysisk) person som är i livet. Om man direkt eller indirekt av den registrerade uppgiften kan förstå vem det handlar om är det fråga om en personuppgift. Personnummer är alltid en personuppgift eftersom det är en direkt utpekande identitetsuppgift. Likaså kan initialer vara en personuppgift om man av anslutande uppgifter kan förstå vem det rör sig om. Ett fotografi där någon finns avbildad och som lagras digitalt är också en personuppgift om man kan se vem bilden föreställer.

4. Vad är en behandling av personuppgift?

Alla former av åtgärder med personuppgifter oberoende av om de utförs automatiserat eller inte, exempelvis: insamling, registrering, organisering, strukturering, lagring, ändring, bearbetning, framtagning, läsning, användning, utlämning, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

5. Personuppgiftsansvarig

Personuppgiftsansvarig är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (Artikel 3 pkt. 7 dataskyddsförordningen).

Datainspektionen har bestämt att inom den kommunala organisationen är varje nämnd personuppgiftsansvarig för sina behandlingar av personuppgifter.

Personuppgiftsansvaret kan även vara delat mellan flera nämnder. Respektive nämnd är då skyldig att se till att dataskyddsförordningens regler följs, och var och en av de berörda nämnderna kan bli skadeståndsskyldiga även om det bara var en som använde uppgifterna på ett felaktigt sätt. Personuppgiftsansvaret blir alltså gemensamt i sådana fall.

6. Dataskyddsombud

Dataskyddsförordningen ställer krav på Huddinge kommuns nämnder att utse ett Dataskyddsombud vars kontaktuppgifter skall offentliggöras och meddelas till Datainspektionen. Huddinge kommuns nämnder har utsett ett gemensamt Dataskyddsombud.

Dataskyddsombudet har en viktig ställning inom kommunen och Huddinge kommun har säkerställt att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgiftsbehandlingar.

Nämnderna stödjer dataskyddsombudet i utförandet av sina arbetsuppgifter genom att tillhandahålla de resurser som krävs, ge tillgång till personuppgifter och behandlingsförfaranden samt upprätthållandet av dennes sakkunskap.

Dataskyddsombudet får ej avsättas och kan ej bli ålagda sanktioner av den personuppgiftsansvarige för att ha utfört sina arbetsuppgifter. Dataskyddsombudet ska vara oberoende och har inom den allmänna verksamheten tystnadsplikt.

7. Laglig grund och samtycke

Behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

- Som ett led i den personuppgiftsansvariges myndighetsutövning, dvs sådana uppgifter som en myndighet enligt lag ska utföra och som har rättsliga effekter för den enskilde som t.ex. ansökan om ekonomiskt bistånd eller bygglov.
- Den registrerade har lämnat sitt samtycke vilket skall vara individuellt, frivilligt och särskilt.
- Behandlingen är nödvändig för att fullgöra ett avtal mellan den personuppgiftsansvarige och den enskilde som t.ex. vid ett anställningsförhållande.
- För att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige som t.ex. att lämna ut uppgifter om anställda till bland annat statliga myndigheter för att redovisa skatter och sociala avgifter beträffande arbetstagarna.
- För att utföra en uppgift av allmänt intresse som t.ex. arkivering, forskning och framställning av statistik.

Offentliga myndigheter har inte rätt att använda intresseavvägning som laglig grund för behandling av personuppgifter.

Enligt dataskyddsförordningen måste de registrerade informeras om den rättsliga grunden för behandlingen. Om uppgifterna hämtas in direkt från den registrerade skall informationen ges vid inhämtning, men om uppgifterna hämtas från annan än den registrerade skall personuppgiftsansvarige lämna information vid senare tillfälle enligt Artikel 14 pkt.3 i dataskyddsförordningen. För att uppfylla informationsskyldigheten ska den personuppgiftsansvarige inkludera information om vilken den tillämpliga rättsliga grunden är i dennes registerförteckning.

Om behandlingen grundar sig på samtycke måste den personuppgiftsansvarige kunna visa att den registrerade har samtyckt. För att ett samtycke ska vara giltigt måste den registrerade ha informerats om ändamålet och att denne när som helst kan återkalla sitt samtycke samt att samtycket har ingåtts på rätt sätt, dvs genom att den registrerade aktivt gör ett val vid samtycke. Om den registrerade återkallar ett meddelat samtycke ska behandlingen upphöra om det inte finns någon annan tillämplig rättslig grund som ger den personuppgiftsansvarige rätten att fortsätta behandlingen.

8. Principer för behandling

För alla behandlingar av personuppgifter finns alltid ett krav på nödvändighet. All behandling av personuppgifter måste uppfylla de grundläggande principer som anges i dataskyddsförordningen. Principerna ska iakttas vid all behandling. Den personuppgiftsansvarige måste ha rutiner för att se till att principerna följs. Mer information om principerna finns nedan i detta avsnitt.

Det bör ifrågasättas om de uppgifter som registreras faktiskt är nödvändiga för ändamålet, t.ex. behövs det sällan ett personnummer på en deltagarlista.

Laglighet, korrekthet (skälighet) och öppenhet (hur behandlas)

All behandling måste ha en rättslig grund för behandlingen och behandlingen ska genomföras i enlighet med dataskyddsförordningen. Det ska vara rimligt och skäligt att behandla personuppgifterna. Behandlingen ska genomföras transparent i förhållande till den registrerade, t.ex. genom att den registrerade ges insyn och information om behandlingen av personuppgifter samt att uppgifterna är lättillgängliga och lättbegripliga samt att ett klart och tydligt språk används.

Ändamålsbestämning och ändamålsbegränsning (för vad)

Att noga och specifikt ange vad som är ändamålet med en behandling av personuppgifter är av stor vikt, bl.a. eftersom ändamålet med behandlingen är avgörande för om behandlingen kan bedömas vara nödvändig eller inte. Personuppgifter får inte behandlas för ändamål som är oförenliga med de ändamål för vilka uppgifterna ursprungligen samlades in.

Uppgiftsminimering (mängd)

Personuppgifter bör vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för. Den personuppgiftsansvarige ska inte samla in mer personuppgifter än vad som är nödvändigt med hänsyn till ändamålet.

Korrekthet (korrekt och uppdaterade uppgifter)

Den personuppgiftsansvarige ska vidta alla rimliga åtgärder för att rätta och uppdatera eller radera felaktiga personuppgifter. Så länge de är felaktiga får de inte behandlas.

Lagringsminimering (tid)

Personuppgifter får inte lagras längre än vad som är nödvändigt. Avgörande för hur länge en personuppgift får lagras eller på annat sätt behandlas är om uppgiften är nödvändig för det ändamål som den behandlas för. Om en personuppgift inte längre behöver behandlas för ett visst ändamål ska den raderas, alternativt föras över till annat system för bevarande. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll.

Principen om lagringsminimering lägger inte hinder i vägen för att Huddinge kommun bevarar och arkiverar allmänna handlingar, eller att arkivmaterial tas om hand av en arkivmyndighet. Detta styrs av arkivlagen och offentlighets- och sekretesslagen.

Integritet och konfidentialitet

Den personuppgiftsansvarige ska säkerställa informationssäkerhet vid behandling av personuppgifter, och har en skyldighet att implementera nödvändiga tekniska och organisatoriska åtgärder för att skydda personuppgifterna från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlas.

Testdata

Personuppgifter i test och utbildningsmiljö ska vara avidentifierad eller anonymiserad

Ansvarsskyldighet
Den personuppgiftsansvarige ansvarar för att de grundläggande principerna för behandling efterlevs.

9. Den registrerades rättigheter

Den personuppgiftsansvarige ansvarar för att säkerställa att den registrerades rättigheter tillgodoses genom informationsplikten och ska informera den registrerade om personuppgiftsbehandlingen. Information som skall ges till den registrerade är bl.a. följande:

- Uppgifter om personuppgiftsansvarige och dataskyddsombudet
- Ändamålen med behandlingen
- Rättslig grund för behandlingen
- Vilken kategori av personuppgifter som behandlas
- Till vem personuppgifterna kan komma att lämnas ut
- All tillgänglig information om varifrån uppgifterna kommer, om personuppgifterna inte samlas in från den registrerade
- Om det är frivilligt för den registrerade att lämna uppgifter
- Uppgift om rätten att begära registerutdrag
- Uppgift om lagringstiden eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period
- Uppgift om den personuppgiftsansvariges plikt att vid begäran radera, begränsa eller invända mot behandling eller korrigera felaktiga, ofullständiga eller missvisande personuppgifter
- Information om personuppgifterna kan komma att överföras till ett tredje land och i så fall information om vad som utgör grund för överföringen samt vilka skyddsåtgärder enligt Artikel 46 dataskyddsförordningen som har vidtagits vid överföringen
- Uppgift om den registrerades rätt att lämna klagomål till en tillsynsmyndighet
- Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav
- Om det förekommer eller kan förekomma automatiserat beslutsfattande, inklusive profilering, information om logiken bakom samt den registrerades rätt till att göra invändning
- Rätt till dataportabilitet, vilket innebär att den registrerade har rätt till överföring av personuppgifter direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt

- Den personuppgiftsansvarige ska vid begäran förse den registrerade med en kopia av de personuppgifter som är under behandling
- Personer som önskar ett registerutdrag kan begära det via en e-tjänst på kommunens hemsida. För hantering av registerutdrag ska kommungemensam rutin följas

Om det kommer in begäran om utlämnande av allmänna handlingar till en nämnd så får man inte bortse från sekretessbestämmelsen i 21. Kap. 7 § Offentlighets- och sekretesslagen (OSL). Enligt den ska mottagaren bedöma om denne tror att eventuella personuppgifter som begärs ut, kommer att behandlas i strid med dataskyddslagstiftningen. I sådana fall råder det sekretess för uppgifterna och de ska inte lämnas ut. Den bedömningen är inte alldeles lätt att göra. Vägledning kan fås av kommunjuristen inom kommunstyrelsens förvaltning.

10. Personuppgiftsbiträdesavtal

Dataskyddsförordningen ställer krav på skriftligt avtal när ett personuppgifts-biträde ska behandla personuppgifter för en personuppgiftsansvarigs räkning. Skyddet för behandlade individers personliga integritet är av stor etisk betydelse för Huddinge kommun. Syftet med personuppgiftsbiträdesavtalet är att skydda registrerades personuppgifter.

Systemleverantör, support eller utförare som behandlar personuppgifter åt nämnden är exempel på personuppgiftsbiträden. Personuppgiftsbiträden behöver inte lagra personuppgifterna utan det räcker att den externa parten har tillgång till den personuppgiftsansvariges data för att räknas som ett personuppgiftsbiträde.

I Huddinge kommun används SKLs mall för personuppgiftsbiträdesavtal. Den aktuella versionen tillhandahålls på kommunens intranät

En bedömning bör göras från fall till fall huruvida en leverantör är ett personuppgiftsbiträde eller personuppgiftsansvarig. Detta är särskilt viktigt att tänka på i upphandlingar när förfrågningsunderlaget utformas. Exempel på leverantörer som skulle kunna anses vara personuppgiftsansvariga är rekryteringsbolag som utför bakgrundskontroller genom särskilda metoder och processer, inkassoverksamhet samt revisionsbolag. Om en leverantör anses vara gemensamt personuppgiftsansvarig med Huddinge kommun så bör ett avtal tecknas mellan parterna om respektive parts roller och förhållande gentemot de registrerade.

11. Registerförteckning

Personuppgiftsansvariga är skyldiga att föra en registerförteckning över behandlingar av personuppgifter. Dessa register ska upprättas skriftligen, hållas uppdaterade och vara i elektronisk form. Registerna förvaras i kommunens projektstyrningsverktyg Antura. På begäran ska registret göras tillgängligt för Datainspektionen. Hos en personuppgiftsansvarig ska registret innehålla följande uppgifter:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
- I tillämpliga fall, överföringar av personuppgifter till ett tredje land eller internationell organisation.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.
- Om personuppgifterna behandlas automatiserat.

12. Tekniska och organisatoriska säkerhetsåtgärder

Personuppgiftsansvariga ska skydda registrerades personuppgifter med tekniska och organisatoriska säkerhetsåtgärder som säkerställer en lämplig säkerhetsnivå, med beaktande av behandlingens art, risker och övriga omständigheter. Den personuppgiftsansvarige säkerställer, inbegripet, när det är lämpligt;

- pseudonymisering och kryptering av personuppgifter,
- förmågan att kontinuerligt säkerställa konfidentialitet, riktighet, tillgänglighet, spårbarhet och motståndskraft hos verksamhetssystem och tjänster,
- förmågan att återställa tillgängligheten och tillgången till personuppgifter vid en fysisk eller teknisk incident, samt
- ett förfarande för att kontinuerligt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatorisk åtgärder som säkerställer behandlingens säkerhet.

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Den personuppgiftsansvarige och personuppgiftsbiträdet vidtar åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

För varje verksamhetssystem ska finnas en utsedd systemägare som i samråd med Dataskyddsombudet säkerställa kraven på tekniska och organisatoriska säkerhetsåtgärder.

Personuppgiftsincident

Den personuppgiftsansvarige ska rapportera till Datainspektionen i händelse av en säkerhetsincident beträffande personuppgifter. Detta görs via den rutin för anmälan av personuppgiftsincident som finns på kommunens intranät. Personuppgiftsincidenten ska dokumenteras och anmälas till Datainspektionen inom 72 timmar från det att incidenten kom till kommunens kännedom. Om det är en leverantör (dvs ett personuppgiftsbiträde) som upptäcker incidenten måste den skyndsamt rapporteras till kommunen (dvs informationsägaren). Därefter har kommunen 72 timmar på sig att rapportera till Datainspektionen. I vissa fall ska den registrerade informeras, exempelvis vid risk för att den registrerade utsätts för diskriminering, id-stöld, bedrägeri eller annan ekonomisk förlust.

Konsekvensbedömning

Konsekvensbedömning ska genomföras om en personuppgiftsbehandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Inför en upphandling där personuppgifter kan komma att behandlas ska en konsekvensbedömning genomföras för att kunna säkerställa rätt skydd.
Om personuppgiftsbehandlingen leder till en hög risk ska personuppgiftsansvarige omgående kontakta dataskyddsombudet.

13. Information på webbplatsen

På Huddinge kommuns hemsida, www.huddinge.se, framgår det hur kommunen använder personuppgifter om sina registrerade, om uppgifterna lämnas ut till någon annan, när de gallras, varför man använder personnummer etc.

Personuppgifter om enskilda får endast publiceras på kommunens webbsidor, interna så väl som externa, om det finns rättslig grund för det. Känsliga eller extra skyddsvärda personuppgifter får aldrig publiceras på webben. Om det är ovisst om en situation är integritetskränkande är det lämpligt att inhämta samtycke från den registrerade innan publicering av uppgifterna.

- Att publicera foton på anställda på hemsidan kräver i regel samtycke från den anställde.
- Det finns dock undantag där en intresseavvägning gör det tillåtet att publicera foton.
- Vårdnadshavare måste samtycka innan en publicering av barn sker på hemsidan. Samtycket ska inhämtas från båda vårdnadshavarna.

  Det är viktigt att observera att det kan finnas enskilda med skyddade personuppgifter som skall beakta att krav på starka säkerhetsåtgärder vidtas för det fall att sådana extra skyddsvärda personuppgifter på något sätt registreras så att de finns att nå via internet, exempelvis efter inloggning.

14. Användning av Internet och e-post, telefoni med mera

Huddinge kommun har upprättat nedanstående principer och informerat alla anställda om vad som är tillåtet respektive otillåtet när det gäller hur de anställda använder sin e-postlåda, surfar på Internet, använder telefoni och andra

elektroniska spår som inpasseringssystem och GPS, och hur övervakningen kan komma att ske. E-post sparas i ett år för att säkerställa utredningar om så kommer behövas

Riktlinjerna finns beskrivna i HKF 9820 Riktlinjer för användning av internet, e-post och mobila enheter.

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

- sekretessbelagd information enligt offentlighets- och sekretesslagen, t.ex. hälsoinformation, skyddade identiteter, information som rör Sveriges säkerhet, handlingar som omfattas av upphandlingssekretess, krisberedskapsinformation
- integritetskänsliga och extra skyddsvärda uppgifter, t.ex. personnummer, fotografier på barn, bedömnings- och utvecklingssamtal, boklån, orosanmälningar, uppgifter om lagöverträdelse, löneuppgifter med känsliga personuppgifter, uppgifter om sociala förhållanden: samt
- känsliga personuppgifter, t.ex. etniskt ursprung, politiska åsikter, religiösa övertygelser, facktillhörighet, uppgifter om hälsa, uppgifter om sexualliv/sexuell läggning.

Inga känsliga eller extra skyddsvärda personuppgifter får skickas via e-post.

I det fall man ändå behöver skicka e-post med känsliga personuppgifter eller sekretessbelagd information i sin helhet så krävs att särskilda säkerhetsåtgärder vidtas. Med säkerhetsåtgärder avses i praktiken krypteringsskydd på ett sådant sätt att endast den avsedda mottagaren kan ta del av dem.

I det fall e-post inkommer med känsliga personuppgifter eller sekretessuppgifter?

Om någon skickar känsliga personuppgifter eller sekretessuppgifter så innebär det inte att hen gett sitt samtycke till att hantera personuppgifter per e-post. Den enskilde har ingen information om huruvida kommunens e-post är krypterad eller ej och ett samtycke är därför inte aktuellt. Det är därför viktigt att inte svara genom att skicka med det innehåll som omfattas av sekretess. Dessa uppgifter måste tas bort i svarsmeddelandet och raderas i e-postsystemets inkorg och papperskorg

15. Riktlinje för fritextfält

Den personuppgiftsansvarige ska vara medveten om vilka fritextfält som finns i systemen och vilken målgrupp de exponeras för. Grundprincipen ska vara att inte skapa fler fritextfält än nödvändigt. Syftet med fritextfälten ska framgå och det behöver finnas en teknisk lösning eller rutin för gallring. Verksamheterna ska uttrycka sig professionellt, sakligt, i relation till den specifika frågan, och i övrigt överensstämmande med god etik samt gällande lagar och förordningar.

16. Arkiveringsregler inom Huddinge kommun

Enligt dataskyddsförordningen är behandling av personuppgifter för arkivändamål tillåten och ska regleras enligt nationell lagstiftning. Det innebär att det är arkivlagens regler som gäller när det rör sig om hanteringen av allmänna handlingar. Grundprincipen i arkivlagen är att alla allmänna handlingar ska hållas ordnade och sökbara under sin livstid och att de ska bevaras för all framtid. Undantag från bevarande kan göras av olika skäl. Om handlingen (dvs. uppgiften/informationen) inte ska bevaras ska den gallras. Gallring måste alltid föregås av ett beslut. För kommunens del innebär det att varje nämnd så som personuppgiftsansvariga ska fatta beslut om gallring av uppgifter i allmänna handlingar. Det beslutet fattas i och med att nämnden antar dokumenthanteringsplanerna. Gallringen kan omfattas av gallringsfrister, dvs. att handlingen/informationen ska finnas kvar i t.ex. fem år för att sedan gallras. Handlingar som ska bevaras ska avskiljas från de handlingar som ska gallras så att ingen sammanblandning kan ske, detta kan i ett IT-system t.ex. ske genom metadata.

Enligt dataskyddsförordningen får personuppgifter endast lagras så länge som det är relevant för syftet till behandlingen. (lagringsminimering). Det innebär att även om informationen ska bevaras eller omfattas av en längre gallringsfrist, så måste den lyftas ut ur/separeras från det sammanhang där den ursprungligen lagrades. Detta kan göras genom att åtkomsten till informationen begränsas, t.ex. genom behörighetsstyrning, eller att den flyttas över till ett annat IT-system, t.ex. ett e-arkiv. När en sådan separering ska ske regleras genom dokumenthanteringsplanerna.

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

- Avidentifiering 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 personuppgifterna innebär att se till at de inte går att återskapa. Det är viktigt att känna till vad som krävs rent tekniskt för att uppgifterna verkligen ska förstöras. Det är t.ex. inte tillräckligt att radera filen som innehåller personuppgifterna. Filen kan t.ex. ligga kvar i datorns s.k. ”papperskorg”. I stället krävs säker omformatering av lagringsmediet eller total överskrivning så att personuppgifterna inte kan tolkas i efterhand.

  Personuppgifter i allmänna handlingar får alltså inte förstöras även om den registrerade själv vill det. Enda tillfället då en registrerad kan begära att dennes personuppgifter raderas inom offentlig förvaltning är när insamlingen skett genom samtycke vilket bygger på frivillighet.

17. Personnummer

Det finns inte något förbud mot att registrera personnummer eller samordningsnummer (samordningsnummer är ett unikt identifikationsnummer som kan tilldelas personer som inte är eller har varit folkbokförda i Sverige). Även om ett personnummer inte är en känslig personuppgift så betraktas den som extra skyddsvärd och därför får personnummer inte användas hur som helst.

Det bör alltid övervägas om det är nödvändigt att notera personnummer och andra personuppgifter på alla ställen eller om det räcker med att det finns tillgängligt till exempel i en akt eller enbart i en grunddatabas.

Personnummer ska enbart användas om:

- den registrerade har samtyckt till registreringen,
- behandlingen är klart motiverad med hänsyn till ändamålet med behandlingen (räcker det med anställningsnummer, namn och adress, födelsedatum eller födelseår),
- behandlingen är klart motiverad med hänsyn till vikten av en säker identifiering, t.ex. som grunddata i ett löneadministrativt IT-system, för redovisning av källskatter, vid rehabiliteringsutredning eller kommunikation med skoladministrativt IT-system eller om;
- behandlingen är klart motiverad med hänsyn till något annat beaktansvärt skäl.

Personnummer som användaridentitet vid inloggningar ska undvikas. Om det finns behov av att använda personnummer som inloggning behövs samråd med kommunens dataskyddsombud.

18. Sociala medier

Vid publicering av personuppgifter i sociala medier (Facebook, Twitter, Insta gram, Youtube m.fl.) finns ett ansvar att:

- inte publicera kränkande personuppgifter,
- hålla regelbunden uppsikt över publiceringar för att upptäcka kränkande personuppgifter,
- skyndsamt ska ta bort kränkande personuppgifter, samt att
- vidta lämpliga säkerhetsåtgärder, i form av instruktioner till de som arbetar med sociala medier för kommunens räkning, anställda och andra som agerar på uppdrag av kommunen.

Det som framgår under kapitel 13 avseende publicering av foto gäller även för sociala medier.