Riktlinjer

Datum
2018-04-06

KS 110-2018:20

Godkänd/ansvarig
Fastställd av KS
2018-05-14, § 115

Hantering av personuppgifter i Svalövs kommun

I kommunen hanterar vi en mängd personuppgifter. Det kan handla om personuppgifter om medarbetare, elever, enskilda som söker bygglov eller ekonomiskt bistånd och så vidare. När vi hanterar personuppgifter så behöver vi säkerställa att kommunens hantering är i enlighet med gällande lagstiftning. I denna guide får du som medarbetare information om vad som är viktigt att tänka på när du hanterar personuppgifter.

Dataskyddsförordningen (även kallade GDPR) är ett regelverk för behandling av personuppgifter som har tagits fram av EU. Ett av syftena med lagstiftningen är att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas.

I skrivande stund pågår ett flertal utredningar om hur nationell lagstiftning ska anpassas till den nya dataskyddsförordningen, därför är att svårt att säga exakt hur vissa verksamhetsområden påverkas av den nya lagen. Dessa riktlinjer är därför ett levande material som kommer att uppdateras kontinuerligt framöver.

Innehåll

1. När är det tillåtet att behandla personuppgifter?

Vid behandling av personuppgifter ska man tänka på följande:

1. Personuppgifter ska behandlas på ett **lagligt, korrekt och öppet** sätt i förhållande till den registrerade.

Med öppet sätt avses att det för de registrerade bör vara klart och tydligt hur uppgifter som gäller dem insamlas och används samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av personuppgifter är lättillgänglig och lättbegriplig.

2. Insamlingen av personuppgifter ska vara **begränsad till ändamålet** och ske för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifterna får inte senare användas för ett ändamål som inte är bundet till ändamålet med de insamlade uppgifterna.

Det har ändå ansetts att om uppgifterna senare används för arkivändamål eller för historiska forskningsändamål eller statistiska ändamål gäller inte principen om ändamålsbegränsning.

3. Insamlingen av personuppgifter ska vara **uppgiftsminimerad,** dvs. inte för omfattande i förhållande till de ändamål för vilka uppgifterna behandlas, och uppgifterna ska vara adekvata och relevanta.

Personuppgifter bör behandlas endast om syftet med behandlingen inte rimligen kan uppnås genom andra medel.

4. Personuppgifterna ska vara **korrekta och om nödvändigt uppdaterade**. Den personuppgiftsansvarige ska med rimliga åtgärder säkerställa att personuppgifter som är inexakta och felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

Den personuppgiftsansvarige ska, till exempel med hjälp av fastställda tidsfrister, säkerställa att personuppgifter inte förvaras längre än nödvändigt.

5. Personuppgifter ska f**örvaras** i en form som möjliggör identifiering av den registrerade **endast under den tid som är nödvändig** för de ändamål för vilka personuppgifterna behandlas. Uppgifter får dock förvaras längre, om de endast behandlas för arkivändamål av allmänt intresse, eller används för historiska forskningsändamål eller statistiska ändamål.

6. Personuppgifter ska behandlas på ett sätt som säkerställer **lämplig säkerhet** för uppgifterna och därmed uppgifternas integritet och konfidentialitet.

Uppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Då ska lämpliga tekniska eller organisatoriska åtgärder användas.

1.1. Grunder som tillåter behandling av personuppgifter

• Samtycke - Den registrerade har lämnat sitt **samtycke** till att dennes personuppgifter behandlas av kommunen för ett eller flera specifika ändamål.

Det finns däremot flera undantag från denna utgångspunkt vilket medför att personuppgifter får behandlas utan samtycke om det finns en rättslig grund för det. Vid följande situationer är det tillåtet att behandla personuppgifter utan samtycke:

• Avtalssituation – Behandling av personuppgifter är nödvändig för att uppfylla ett **avtal** mellan den personuppgiftsansvarige och den enskilde. Exempel: Behandlingar för administration av kundförhållande eller anställningsförhållande.

• Rättslig **skyldighet** - Behandling av personuppgifter har stöd av annan författning. Exempel: Lämna ut uppgifter om anställda till bland annat statliga myndigheter för att redovisa skatter och sociala avgifter beträffande arbetstagarna.

• Intressen av grundläggande betydelse för den registrerade - Behandling av personuppgifter är tillåten om det handlar om sådana **intressen** som är av avgörande betydelse för den registrerades eller någon annan persons liv. Som exempel kan nämnas personuppgiftsbehandling som är nödvändig för livsavgörande vård i akuta situationer då den registrerade inte kan lämna samtycke. Detta är en ovanlig rättslig grund för kommunal verksamhet.

• Allmänt intresse - Gäller när behandling av personuppgifter är nödvändig för att utföra en uppgift av **allmänt intresse**. Exempel: Arkivering, forskning och framställning av statistik.

• Myndighetsutövning - Behandling av personuppgifter är tillåten om det är nödvändigt för **myndighetsutövning**. Med myndighetsutövning menas här sådana uppgifter som en myndighet enligt lag ska utföra och som har rättsliga effekter för den enskilde. Observera att detta inte innebär att alla personuppgiftsbehandlingar i en myndighet sker på denna grund, exempelvis är personaladministrativa åtgärder fortfarande en avtalssituation. Exempel: Ansökan om ekonomiskt bistånd eller bygglov.

• Berättigade intressen - behandlingen är **nödvändig** för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade 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.

Observera att grunden ”Intresseavvägning” (enligt personuppgiftslagen) inte längre är tillämplig för myndigheter i den nya dataskyddsförordningen.

2. Personuppgifter i e-post

E-post är en av flera typer av personuppgiftsbehandlingar. Enligt PuL (personuppgiftslagen) föll e-post under undantaget för ostrukturerade personuppgifter. Någon laglig grund behövdes alltså inte för att behandla personuppgifter i e-post. Enligt den nya dataskyddsförordningen upphör detta undantag och det krävs en laglig grund för behandling av personuppgifter i e-post.

2.1. Grund för behandling i e-post

En stor del av den personuppgiftsbehandling som förekommer i de kommunala myndigheternas e-post kan hänföras till den lagliga grunden ”arbetsuppgifter av allmänt intresse” såvida innehållet eller ämnet berör de arbetsuppgifter myndigheten har att fullgöra inom ramen för den kommunala kompetensen. Det kan till exempel röra sig om e-post i bygglovsärenden med invånare.

Även den lagliga grunden ”rättslig skyldighet” kan läggas till grund för behandling av personuppgifter i sådan e-post, till exempel enligt dokumentationskravet i förvaltningslagen eller annan speciallagstiftning.

Inom den verksamhet som kommuner bedriver frivilligt den lagliga grunden ”intresseavvägning” använts denna grund har upphört i och med den nya dataskyddsförordningen. Regeringen har därför ansett att begreppet uppgifter av allmänt intresse ska ges en vidare betydelse (prop. 2017/18:105 s. 56). Med stöd av den lagliga grunden uppgifter av allmänt intresse kan myndighet således behandla personuppgifter inom den frivilliga verksamheten, om behandlingen är nödvändig, till exempel e-post inom kultur- och

idrottsförvaltningen. Likaså för dagliga administrativa funktioner och åtgärder i den kommunala förvaltningen (prop. 2017/18:105 s. 61), till exempel e-post till och från kontaktpersoner hos leverantörer eller liknande.?

2.2. Personuppgifter som inte ska skickas i e-post?

I dagsläget är inte kommunens e-post krypterad vilket innebär att vi inte ska skicka känsliga eller extra skyddsvärda personuppgifter via mejl[1].

• Uppgifter som hör till känsliga personuppgifter är till exempel hälsoinformation (se fler exempel i avsnittet ”Definitioner” och känsliga personuppgifter).

• Extra skyddsvärda uppgifter är till exempel sekretessbelagd information enligt offentlighets- och sekretesslagen eller personnummer (se fler exempel i avsnittet ”Definitioner” och extra skyddsvärda personuppgifter).

Om du avidentifierar innehållet så kan du däremot skicka uppgifterna, det förutsätter dock att mottagaren förstår vem information berör.

I de fall vi ändå behöver skicka e-post som innehåller uppgifter som hör till 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. Vissa e-postsystem har funktioner för att kryptera meddelanden mellan användare inom samma e-postdomän men vanligtvis behövs särskilda krypteringsnycklar eller programvaror för att kryptera e-post. Ta reda på vad som gäller om du måste skicka dessa kategorier av personuppgifter!

2.3. Arbetar du inom hälso- och sjukvården?

Inom hälso- och sjukvården gäller särskilda bestämmelser utifrån Socialstyrelsens föreskrifter - Informationshantering och journalföring inom hälso- och sjukvården. Föreskrifterna innehåller bestämmelser om hantering av patientuppgifter över öppna nät som innebär att överföring av patientuppgifter ska göras på ett sådant sätt att ingen obehörig kan ta del av uppgifterna. Det gäller även för e-post och innebär i praktiken ett krav på att patientuppgifterna i ett e-post-meddelande ska krypteras på ett sådant sätt att endast den avsedda mottagaren kan ta del av dem.

2.4. Hur gör jag om någon skickar e-post till mig med uppgifter som hör till känsliga eller extra skyddsvärda personuppgifter?

Om någon skickar uppgifter som hör till kategorin 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 inte och ett samtycke är därför inte aktuellt. Tänk därför på att du inte svarar genom att skicka med det innehåll som omfattas av sekretess. Dessa uppgifter måste tas bort i svarsmejlet.

3. Var försiktig med personnummer

Tvärt emot vad många tror, finns det 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 används hur som helst eller utsättas för onödig spridning.

[1] För kommunikation med vissa myndigheter är dock e-posten krypterad.

Överväg alltid om det är nödvändigt att notera personnummer på alla ställen som du har tänkt det, eller om det räcker med att det finns tillgängligt till exempel i en akt eller enbart i en grunddatabas. Det är framförallt den slentrianmässiga användningen av personnummer som man måste vara observant på, exempelvis i mejlkonversationer. Tänk efter; stödjer syftet med behandlingen av personuppgifter att personnummer registreras?

Personnummer ska enbart användas:

• om den registrerade har samtyckt till registreringen,

• om behandlingen är klart motiverat med hänsyn till ändamålet med behandlingen (räcker det med förslagsvis namn och adress, födelsedatum eller födelseår, så ska du nöja dig med det),

• om behandlingen är klart motiverat med hänsyn till vikten av en säker identifiering. Exempelvis är det tillåtet att registrera de anställdas personnummer i ett register som innehåller grunddata eller till exempel ett löneadministrativt IT-system, för redovisning av källskatter, vid rehabiliteringsutredning eller kommunikation med facket i lönerevisioner, i ett kommuninvånarregister och elevers personnummer i ett skoladministrativt IT-system. Personnummer behövs i dessa fall på grund av vikten av en säker identifiering, det vill säga man måste vara säker på vem personen är när man exempelvis sätter betyg, administrerar ansökningar till barnomsorg eller äldreomsorg, i tillsynsärenden på miljöenhet, i kravärenden och när kommunen rapporterar till skatteverket. Enligt socialtjänstregisterlagen och patientdatalagen (skolhälsovård, äldreomsorg, hälso- och sjukvård) är det tillåtet att använda personnummer på grund av vikten av en säker identifiering, i verksamheter som regleras av den lagstiftningen. I en situation när man till exempel lämnar krediter, hyr ut en lokal och ska fakturera eller liknande, har Datainspektionen accepterat att man använder personnummer. Det förefaller även vara tillåtet i biblioteksregister eftersom en utlånad titel kan utgöra ett relativt högt värde (men det finns flera motsägande beslut).

• om behandlingen är klart motiverat med hänsyn till något annat beaktansvärt skäl.

Bestämmelserna om personnummer gäller däremot inte födelsedatum. Datainspektionen har ändå ansett att det är tveksamt om det finns anledning att registrera födelsedatum på till exempel en deltagarlista. Är det inte viktigt när någon fyller år eller hur gammal han eller hon är, behövs ju varken födelsedatum eller födelseår.

3.1. Skillnad på personnummer och födelsedatum

Reglerna om personnummer är tillämpliga när alla 10 (eller 12) siffror används för att identifiera en person. Observera alltså att enbart de sex första siffrorna inte är ett personnummer, utan ett födelsedatum. Födelsedatum kan i och för sig också vara en personuppgift, men många personer är ju födda på samma dag så det pekar i sig inte ut en individ generellt sett. Det skulle däremot kunna göra det om personen finns i en begränsad grupp, till exempel i en skolklass eller på en deltagarlista.

Reglerna om behandling av personnummer gäller även utskrifter, och de gäller även om man har manipulerat numret till exempel genom att det registreras i omvänd nummerordning eller genom att man lagt till siffror framför eller bakom den tiosiffriga (eller tolvsiffriga) kombinationen.

3.2. Personnummer som användaridentitet

Undvik att använda personnummer som användaridentitet vid inloggningar. I stora organisationer med många anställda har Datainspektionen i undantagsfall godtagit användning av personnummer både för behörighetsadministration och

inloggning om det behövs för en säker identifikation av användaren. Om det finns behov av att använda personnummer som inloggning så behövs samråd med kommunens dataskyddsombud.

4. Avidentifierade eller krypterade personuppgifter

Om informationen du har registrerad de facto är avidentifierad så rör det sig inte längre om en behandling av personuppgifter och bestämmelserna i dataskyddsförordningen blir inte tillämpliga. För att personuppgifterna ska anses vara avidentifierade så krävs dock att man inte kan hitta tillbaka till en enskild individ även om man tillför annan information, till exempel en krypteringsnyckel. Det har ingen betydelse om krypteringsnyckel är inbyggd i ett verksamhetssystem eller om den är nedskriven på ett papper, så länge den finns att tillgå så är inte personuppgifterna avidentifierade. Inom statistik och forskning är användningen av avidentifierade uppgifter vanligt då svar och resultat inte går att härleda till en enskild individ.

Kryptering är en teknisk säkerhetsåtgärd men innebär alltså inte att informationen är avidentifierad och därför är dataskyddsförordningen tillämplig även på krypterade uppgifter. I Datainspektionens vägledning kring informationssäkerhet fastställs att uppgifter som hör till känsliga personuppgifter ska vara krypterade vid överföring, exempelvis i mejlkommunikation.

5. Hanterar ett externt företag personuppgifter för kommunens räkning?

Det är vanligt att ett externt företag, som till exempel systemleverantör, support eller utförare, behandlar personuppgifter åt nämnden. Den externa parten kallas då personuppgiftsbiträde. Biträdet finns alltid utanför den personuppgiftsansvariges (nämnden/styrelsens) egen organisation. Observera att det inte alls behöver handla om lagring av personuppgifter, utan det är också en biträdessituation när en extern part har åtkomst till den personuppgiftsansvariges data genom sitt uppdrag för service, support, underhåll, utveckling och liknande. Det är möjligheten att påverka personuppgifterna som är det viktiga, inte var de fysiskt är lagrade i första hand.

En av de stora nyheterna i dataskyddsförordningen är att personuppgiftsbiträdet har ett rättsligt ansvar för den behandling av personuppgifter som utförs för den personuppgiftsansvariges räkning. Det gäller inte alla artiklar i dataskyddsförordningen, och huvudansvaret för behandlingen ligger fortfarande kvar på den personuppgiftsansvarige men dataskyddsmyndigheten har möjlighet att öppna tillsyn mot personuppgiftsbiträdet utan att gå vägen runt kunden.

5.1. Vanliga biträdessituationer

Det är vanligt att biträdessituationer uppkommer för exempelvis personaladministrativa system, kundadministrativa system, lärplattformar, ärendehanteringssystem, passersystem, arkiv- och dokumentdatabaser, bokningssystem, diarier och liknande.

5.2. Ta fram ett biträdesavtal

I alla biträdessituationer ska det finnas ett skriftligt avtal (biträdesavtal) mellan den personuppgiftsansvarige och biträdet. Lagstiftningen ställer stora krav på hur avtalet är utformat så ta hjälp vid utformningen. I avtalet ska villkoras biträdets hantering av personuppgifterna och det är den

personuppgiftsansvarige som är skyldig att se till att skriftliga biträdesavtal finns. Det är oftast enklast och tydligast att ha biträdesavtalet som en del av tjänsteavtalet. Då slipper man göra en separat beskrivning av uppdraget, som kanske senare ändras i tjänsteavtalet utan att någon tänker på att även biträdesavtalet måste ändras på samma sätt.

5.3. Viktigt att tänka på

5.3.1. Åtaganden ska återspeglas i avtal med underleverantörer

Tänk på att personuppgiftsbiträdets egna åtaganden gentemot en personuppgiftsansvarig alltid ska återspeglas i avtal med eventuella underleverantörer.

Enligt dataskyddsförordningen får personuppgiftsbiträdet bara anlita underleverantörer efter att den personuppgiftsansvarige gett sitt godkännande. Detta måste framgå explicit av avtalet. Ett lämpligt tillvägagångssätt är att, i en bilaga till biträdesavtalet, lista alla de underleverantörer som huvudleverantören anlitar i dagsläget, var de finns geografiskt och vilken roll de har i dataprocessen. Godkännandet kan göras generellt när avtalet ingås, men personuppgiftsbiträdet ska sedan underrätta den personuppgiftsansvarige om planerade förändringar och ge denne möjlighet att invända.

5.3.2. Konfidentialitet

I dataskyddsförordningen ställs som krav att alla anställda hos personuppgiftsbiträdet som har åtkomst till personuppgifterna, antingen ska ha åtagit sig en tystnadsplikt eller ha en tystnadsplikt enligt lämplig lag.

5.3.3. Ansvarsfördelning mellan biträde och ansvarig

Det är nödvändigt att personuppgiftsbiträdet bistår uppdragsgivaren (den personuppgiftsansvarige) när det behövs för att uppdragsgivaren ska kunna uppfylla kraven i GDPR. Om en registrerad exempelvis begär att få ta del av information som finns registrerad om denne eller begär rättelse av sådan information, ska biträdet hjälpa till.

5.3.4. Påtala felaktigheter

Personuppgiftsbiträdet har en skyldighet att "omedelbart informera den personuppgiftsansvarige om han anser att en instruktion strider mot denna förordning eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser". Vilka krav detta ställer på personuppgiftsbiträdets kunskap om lagstiftningen får praxis utvisa. Det står dock inte att personuppgiftsbiträdet i sådana fall ska vägra att utföra behandlingen, utan det är rimligtvis den personuppgiftsansvarige som slutligen tolkar lagstiftningen och bestämmer om behandlingen ska genomföras eller inte.

5.3.5. Om personuppgiftsbiträdet använder personuppgifterna på ett felaktigt sätt

Om personuppgiftsbiträdet använder personuppgifterna för sin egen verksamhet, blir biträdet istället personuppgiftsansvarig för den behandlingen. En sådan situation kan uppkomma om personuppgiftsbiträdet är en IT-systemleverantör som använder kundens data för utveckling av sina tjänster. Det är inte tillåtet enligt Datainspektionens praxis och det ska inte finnas med några sådana förutsättningar i ett biträdesavtal.

6. Publicering av personuppgifter på hemsidan

Personuppgifter om enskilda får endast publiceras på hemsidan om det finns laglig grund för det. Tänk på att personuppgifter som enskilt kan betraktas som

harmlösa kan anses som vara kränkande beroende på sammanhanget de publiceras i. Känsliga eller extra skyddsvärda personuppgifter får aldrig publiceras på webben.

6.1. Samtycke är alltid ett bra alternativ för publicering

Är du osäker på om en uppgift kan anses vara integritetskränkande så använd dig av möjlighet att hämta in samtycke. Samtycker den enskilde så kan du publicera uppgifterna. Fyller den enskilde i en ansökan digitalt eller i pappersformat så kan du alltid be om samtycke i samband med ansökan. Viktigt är att alla samtycken, oavsett hur de inhämtas, dokumenteras för att kunna hänvisa till dessa. Läs mer om samtycke i senare avsnitt.

6.2. Offentlighetsprincipen då?

Offentlighetsprincipen och integritetsskyddslagstiftningen (dataskyddsförordningen) har olika syften. 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. Det kan illustreras med nedan exempel:

En nämnd beslutar om att vitesförelägga en privatperson för brott mot miljöbalken. Hur ska beslutet hanteras utifrån:

• Offentlighetsprincipen?

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

• Dataskyddsförordningen?

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

6.2.1. Webbdiarium

Att publicera diarier och protokoll på hemsidan sker inte med stöd av offentlighetsprincipen utan går utöver kommunens skyldighet enligt grundlagen – med det sagt är det heller inte otillåtet att ha ett webbdiarium. För de handlingar som publiceras i webbdiariet gäller däremot dataskyddsförordningen.

Personuppgifter som direkt pekar ut en enskild får inte publiceras i webbdiariet, 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 enskilda uppgifter i handlingarna som ska döljas, inte hela diarieposten i sig.

Observera att uppgifter som hör till särskilda kategorier av personuppgifter får under inga omständigheter publiceras på hemsidan. Tänk på att bara uppgiften om att en enskild förekommer i ett ärende kan vara en känslig personuppgift.

En sekretessmarkering innebär ingen absolut sekretess för uppgiften. Om det kommer in en begäran enligt offentlighetsprincipen om att uppgiften ska lämnas ut, måste kommunen göra en sekretessprövning i varje enskilt fall. Tänk på att uppgiften kan bli offentlig om den tas in i ett protokoll eller ett beslut.

6.3. Särskilt om fotografering

Att publicera foton på anställda på hemsidan kräver i regel samtycke från den anställde. Det finns dock en typ av foton som har en speciell status. Det gäller foton på personal som besöker medborgarna i hemmet. För att man ska kunna

kontrollera att det verkligen är hemtjänstpersonal eller fastighetsskötaren som ringer på dörren och vill bli insläppt, är det tillåtet för kommunen att publicera foton på sådan personal utan föregående samtycke (dock ska de naturligtvis informeras). Även personer i ledande ställning, som tjänstemannaledningen, kan räkna med att få sin bild publicerad på hemsidan.

Inom skola, förskola och fritids måste vårdnadshavare samtycka innan en publicering av barn sker på hemsidan. Samtycket ska inhämtas från båda vårdnadshavarna. Alla bilder på barn är inte att anse som kränkande, men det är större risk att en bild på ett barn anses kränkande än en bild på en vuxen. I dataskyddsförordningen finns en bestämmelser som säger att man ska ta särskild hänsyn till att uppgiften avser ett barn, när man gör en intresseavvägning. Om samtycket utformas på ett korrekt sätt behöver det bara inhämtas en gång för alla bilder som publiceras under hela skoltiden. Med korrekt menas att det täcker det ändamål man har tänkt sig med publiceringen. Det kan alltså vara skillnad på olika slags bilder/motiv. Det kan dock vara säkrare, det vill säga begripligare, om man hämtar samtycken i början av varje läsår.

Det är lätt hänt att foton och filmer av misstag eller oaktsamhet innehåller bilder på den person som har **skyddade personuppgifter**. Speciellt olyckligt blir det om fotot eller filmen publiceras på Internet eller på annat sätt med stor spridning. Här kan det vara bra med en rutin som ser till att foton och filmer används på ett sätt som den aktuella personen/vårdnadshavarna har godtagit.

6.3.1. Fotoarkiv

Det är framförallt publicering av bilder och filmer som kan upplevas som kränkande. Se därför över vilka bilder som finns i sociala medier, lärplattformar, presentationsmaterial och hemsida. Finns det inte ett samtycke som är utformat på det sätt som GDPR kräver måste man överväga att ta bort bilden eller inhämta ett nytt, giltigt, samtycke. Däremot är det inte lika givet att man behöver samtycke för att ha bilder i ett "fotoarkiv". Det finns egentligen ingen anledning att rensa bort alla bilder i ett sådant arkiv, men samtidigt kan man fundera på vad man ska ha dem till om de inte går att använda publikt.

Ett annat problem kan vara att andra personer tar foton på arbetsplatsen eller i skolan och publicerar på sina sociala media. Det finns enkla program för ansiktsigenkänning idag, vilket kan äventyra säkerheten för personen med skyddade personuppgifter. Det är inte helt ovanligt med fotoförbud idag på skolor och daghem - och man behöver inte motivera förbudet särskilt med att det finns personer med speciella skyddsbehov just i den egna verksamheten.

6.4. Särskilt om sociala medier

Användning av sociala medier innebär ofta att personuppgifter behandlas. På Svalövs kommuns intranät finns särskilda riktlinjer för användande av sociala medier, klistra in följ länken i webbläsaren:

http://intranet.svalov.se/policyreglertaxor/informationkommunikation.4.9a4a72112648cefb03800033.html

När Svalövs kommun som organisation publicerar personuppgifter 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 publiceringar för att upptäcka kränkande personuppgifter,

• skyndsamt ska ta bort kränkande personuppgifter,

• vidta lämpliga säkerhetsåtgärder (det innebär bland annat att kommunen ska ge instruktioner till de som arbetar med sociala medier för organisationens räkning, anställda och andra som agerar på uppdrag av kommunen).

I personuppgiftsansvaret ingår det alltså att se till att det hålls en god ton bland besökarna på till exempel kommunens Facebook-sida. För att minska risken för kränkningar av enskildas personliga integritet menar Datainspektionen att den personuppgiftsansvarige också bör vidta åtgärder i förebyggande syfte. Det kan till exempel vara att:

• informera om för vilka ändamål som kommentarsfunktionen är tänkt att användas, vilka typer av kommentarer som inte får förekomma och att publiceringar kan komma att plockas bort,

• uppmana användare att rapportera kränkande innehåll till organisationen och ha rutiner för att hantera klagomål.

6.4.1. Vilket ansvar har organisationen?

Enligt Datainspektionen kan ansvaret för behandling av personuppgifter via sociala medier delas in i ansvaret för organisationens egna inlägg och publiceringar och ansvaret för inlägg som publiceras av besökare.

När det gäller Facebook, Instagram, Google Plus, Flickr, Pinterest, LinkedIn och bloggar (och liknande) är organisationen (dvs kommunen) ansvarig för alla personuppgifter som publiceras på kommunens media. Ansvaret omfattar normalt alltså både personuppgifter som kommunen själv publicerar och personuppgifter som publiceras av andra i till exempel en kommentar. Även den besökare som skrivit en kommentar kan ha ett ansvar för vad den själv skrivit.

Organisationer som använder Twitter ansvarar endast för personuppgifter som organisationen själv publicerat, inte personuppgifter som andra twittrande lämnar. Det beror på att organisationen inte kan påverka publiceringen av andras twitter-inlägg.

För andra sociala medier måste organisationen göra en egen bedömning av vilket ansvar den har för andras publiceringar. Kan organisationen påverka det som besökaren publicerar och därmed bestämma över ändamålen och medlen för den behandling av personuppgifter som andra utför (som för Facebook och bloggar)? Eller kan den det inte (som på Twitter)? Svaret påverkar organisationens ansvar.

7. Gallra personuppgifter

Kortfattat kan det sägas att det är ändamålet, alltså anledningen till att personuppgifterna behandlas, som avgör hur länge uppgifterna får sparas innan de gallras. Ändamålet för behandlingen måste bestämmas redan innan personuppgifterna samlas in och registreras. Ändamålet ska kunna anges uttryckligen. Gallring av personuppgifter ska föregås av ett beslut. Regler om gallring hindrar dock inte att en myndighet (nämnden), arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet.

Bestämmelserna om allmänna handlingar enligt offentlighets- och sekretesslagen har då företräde framför bestämmelserna i dataskyddsförordningen.

7.1. Hur tar man bort 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. Det är viktigt att känna till vad som krävs rent tekniskt för att uppgifterna verkligen ska förstöras. Det är till exempel inte tillräckligt att radera den fil som innehåller personuppgifterna. Det är nämligen inte säkert att ett sådant kommando verkligen raderar all information, filen kan exempelvis ligga kvar i datorns "papperskorg". I stället krävs säker omformatering av lagringsmediet eller total överskrivning så att personuppgifterna inte kan tolkas i efterhand. Det är däremot inte heller säkert att vanlig formatering raderar alla uppgifter utan det kan krävas särskild utrustning eller specialprogramvaror. Hur långtgående tekniska åtgärder som bör vidtas är bland annat beroende av informationens känslighet.

Exempel 1: Är ändamålet bara att kunna veta vilka personer som finns i huset och var, vid en eventuell evakuering, är gallringstiderna förstås väldigt korta. Ändamål som att känna igen personens namn nästa gång hen kommer, och föreslå mottagarnamn, kräver normalt samtycke, vilket kan vara lite krångligt att administrera. Tänk på att lämna kort information om registreringen till exempel på startsidan (det görs väldigt sällan i besökssystem men är ett krav).

Exempel 2: Personuppgifter som inkommer i en rekryteringsprocess (ansökan, intervjuanteckningar och uppgifter referenser) bör normalt gallras bort när anställningsförfarandet har avslutats. Arbetsgivaren får däremot uppgifterna så länge den sökande till exempel har möjlighet att överklaga beslutet om att denne inte fick jobbet. Vill arbetsgivaren använda uppgifterna längre, till exempel för framtida rekrytering, måste den arbetssökande informeras och samtycka till fortsatt registrering. För uppgifter om den som blivit anställd gäller andra gallringsfrister.

7.2. Dokumenthanteringsplanen anger när det ska gallras

Är du osäker på när en handling ska gallras (och tillhörande personuppgifter) så anges gallringsfristen i den dokumenthanteringsplan som varje nämnd antagit. Ingen handling får gallras utan ett att beslut har fastställts i en dokumenthanteringsplan.

Dokumenthanteringsplanen gäller både för digitala handlingar och fysiska handlingar. Av dokumenthanteringsplanen framgår även om speciallagstiftning anger särskild gallringsfrist (till exempel patientdatalagen).

8. Varje behandling av personuppgifter ska anmälas till dataskyddsombudet

Behandlingar av personuppgifter ska anmälas till kommunens dataskyddsombud. I princip innebär det att all **helt eller delvis automatiserad behandling** av personuppgifter ska anmälas till ombudet. Vanligtvis rör det sig om behandling av personuppgifter i digitala verksamhetssystem, men även **manuella register** i exempelvis pärmar eller annan strukturerad samling av personuppgifter ska anmälas. Se vidare nedan under ”Definitioner” Helt eller delvis automatiserad behandling och manuella register.

Förteckningen är en förutsättning för att kommunen ska kunna fullgöra sin skyldighet att lämna registerutdrag till den som efterfrågar det. Förteckningen ger också viktig information över hur dataflödena ser ut inom kommunen och

hur kommunen efterlever lagstiftningen. Det är därför av stor vikt att alla nya behandlingar anmäls till dataskyddsombudet.

8.1. Hur anmäler jag en behandling?

Du anmäler en personuppgiftsbehandling genom att besvara ett webbaserat formulär i systemet Draftit. För att få tillgång till formuläret måste du kontakta personuppgiftsassistenten eller dataskyddsombudet inom din verksamhet som ser till att du får en länk skickad till dig. Följ länken och besvara frågorna. Spara gärna länken eftersom du då lätt kan gå tillbaka till formuläret och ändra eller uppdatera information. Om du tappar bort länken så kontakta personuppgiftsassistenten för hjälp.

Genom att anmäla behandlingen i god tid innan behandlingen sätts igång har du tid att säkra att behandlingen sker i enlighet med dataskyddsförordningen. Det är ofta i samband med anmälan som det är lätt att upptäcka om det finns brister när det gäller hanteringen. Kanske behöver säkerheten för personuppgifterna ses över ytterligare eller ett samtycke inhämtas med den enskilde. När det gäller uppgifter som hör till särskilda kategorier av personuppgifter så kan en särskild konsekvensbedömning behöva genomföras innan behandlingen påbörjas.

9. Vilka säkerhetskrav ska ställas på en personuppgiftsbehandling?

För alla som hanterar och bearbetar personuppgifter är det viktigt att säkerställa att personuppgifterna skyddas på ett bra sätt. Den personuppgiftsansvarige måste vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna. Tekniska åtgärder omfattar saker som brandväggar, krypteringsfunktioner och anti-virus, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation, rutiner och styrdokument. Observera att behandling av känsliga och extra skyddsvärda personuppgifter ställer högre krav på vidtagna säkerhetsåtgärder.

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

• Omfattas uppgifterna av tystnadsplikt eller sekretess enligt offentlighets- och sekretesslagen eller annan lagstiftning?

• Omfattas behandlingen av någon särlagstiftning, till exempel patientdatalagen eller lagen om behandling av personuppgifter inom socialtjänsten med flera?

• Är det uppgifter om lagöverträdelser?

• Är det uppgifter om enskildas personliga förhållanden?

Är svaret Ja på någon av dessa frågor ska säkerhetsåtgärderna för att skydda personuppgifterna vara mer omfattande.

9.1. Konsekvensbedömning

Att genomföra en konsekvensbedömning för en särskild personuppgiftsbehandling är en bra utgångspunkt för att säkerställa en säker och korrekt behandling. I konsekvensbedömningen tar den personuppgiftsansvarige ställning till lämpliga säkerhetsåtgärder, risker och konsekvenser samt bedömer hur känsliga de behandlade uppgifterna är.

Frågor som ställs i en konsekvensbedömning:

• 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?

• 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?

• Hur stor är sannolikheten för och konsekvenserna av tekniska störningar eller att obehöriga får åtkomst till uppgifterna?

Ju fler av dessa frågor som man svarar Ja på desto mer omfattande bör säkerhetsåtgärderna vara. Åtgärder som vidtas ska bidra till en adekvat säkerhetsnivå som är lämplig i förhållande till tillgänglig teknik, kostnader, de särskilda riskerna med behandlingen och hur pass känsliga uppgifterna är.

Enligt dataskyddsförordningen har den personuppgiftsansvarige en skyldighet att genomföra en konsekvensbedömning, en typ av risk- och sårbarhetsanalys, för varje ny behandling av uppgifter som hör till särskilda kategorier av personuppgifter. Konsekvensbedömningen är ett effektivt hjälpmedel för den personuppgiftsansvarige att säkerställa en korrekt och säker behandling av personuppgifter. Tänk på att dokumentera resultatet från konsekvensbedömningen. Ta hjälp av dataskyddsombudet för råd om när en konsekvensbedömning ska göras så är hen delaktig i genomförandet av den.

9.2. Att arbeta på distans – tänk på det här

Respektive sektorschef avgör om det är tillåtet med distansarbete och dokumenterar om det finns några särskilda reservationer eller regler för detta. Det är viktigt när du arbetar på distans att du tänker på hur du behandlar eventuella personuppgifter i ditt arbetsmaterial. All verksamhetsrelaterad information ska lagras på ett personligt (W:/) eller gemensamt (T:/) diskutrymme. I skydd av åtkomstbegränsning och med utökad spårbarhet kan även känslig eller sekretessbelagd information lagras på samma plats. Använd alltså inga andra lagringsytor för ditt arbetsmaterial (till exempel Dropbox, Google Drive eller liknande). För delning av dokument hänvisas till Flir. Använd inte heller din privata e-postadress för att kommunicera med kollegor i tjänsten.

Begränsningen av hur och var arbetsrelaterad information, inklusive personuppgifter, lagras är en del av Svalövs informationssäkerhetspolicy.

Du kan läsa mer om policyn genom att följa denna länk:
http://intranet.svalov.se/download/18.7acaab8714f420dd73f437aa/1444123320340/Informationss%C3%A4kerhetspolicy.pdf

10. Skyddade/sekretessmarkerade personuppgifter

Om någon är utsatt för ett allvarligt hot kan Skatteverket besluta om skyddade personuppgifter i särskilda fall. Det finns tre typer av skyddade personuppgifter. Den högsta nivån, den med högst säkerhetsnivå, är att man får en ny identitet, det vill säga fingerade personuppgifter i folkbokföringen. Sedan kommer kvarskrivning, det vill säga att man kvarstår som folkbokförd på sin gamla adress. Det vanligaste är att man får en sekretessmarkering i folkbokföringen, den så kallade folkbokföringssekretessen. Det finns inga generella rekommendationer kring hanteringen av skyddade personuppgifter därför är rekommendationen att man alltid frågar den berörde själv (kan vara en anställd) eller vårdnadshavarna om hur de vill att deras personuppgifter ska hanteras.

När det gäller behandling av skyddade personuppgifter ska den personuppgiftsansvarige, utöver att se till att behandlingen följer dataskyddsförordningen, även tänka på följande:

• Regler och rutiner ska finnas för att säkerställa att skydda personuppgifter behandlas på ett sådant sätt att det inte innebär en ökad risk för registrerade.

• En riskbedömning ska göras från fall till fall då behovet av vilka uppgifter som behöver särskilt skydd varierar.

• Vid behandling av skyddade personuppgifter är det extra viktigt att endast registrera uppgifter nödvändiga för ändamålet, dessa ska även gallras så snart de inte längre behövs.

• Den personuppgiftsansvarige bör begränsa åtkomsten till de skyddade personuppgifterna till ett fåtal personer. För de personer som har åtkomst till uppgifterna ska det också tydligt framgå att de är skyddade (exempelvis genom flaggning).

• Den personuppgiftsansvarige bör se till att skyddade personuppgifter inte okontrollerat sprids mellan olika verksamhetssystem som utbyter data. Det är alltså viktigt att skyddade personuppgifter inte sprids till ett system med sämre säkerhet. Den personuppgiftsansvarige är skyldig att vidta lämpliga säkerhetsåtgärder (med hänsyn till den konsekvensbedömning som gjorts avseende behandlingen).

• All personal som kommer i kontakt med skyddade personuppgifter måste få kunskap om de regler och rutiner som gäller.

• Se till att verksamhetssystem som behandlar skyddade personuppgifter genererar loggar så att det i efterhand går att kontrollera vem som har haft tillgång till informationen. Glöm inte att följa upp och kontrollera loggarna!

10.1. Olika regler i olika förvaltningar

Observera alltså att det föreligger sekretess för så kallade skyddade adresser i folkbokföringen, men sekretessen överförs inte från kommunernas befolkningsregister till de kommunala förvaltningarnas administrativa register. Adressen kan omfattas av annat sekretesskydd vid förvaltningen. Ett exempel är att det råder sekretess inom socialtjänsten för uppgift om enskilds personliga förhållanden, men vid flera kommunala förvaltningar saknas bestämmelser om sekretess som kan omfatta den enskildes personuppgifter. För att spärrmarkerade personuppgifter som förekommer i kommunal verksamhet ska kunna skyddas är det därför nödvändigt att dessa uppgifter endast registreras i kommunens befolkningsregister, i administrativa register i verksamheter där de omfattas av någon form av verksamhetsspecifik sekretess eller där en allmän sekretessregel kan tillämpas.

Det är viktigt att man inte indirekt avslöjar att en person bor i kommunen genom att på en fråga svara något i stil med "Det kan jag inte säga". Man får helt enkelt säga att man inte har någon uppgift om att personen ifråga skulle bo i kommunen. För redan uppgiften om att en person bor i en viss kommun gör det enkelt för den som verkligen vill, att hitta henne eller honom, även om den inte fått reda på den exakta adressen. Vi måste dock göra en reservation för vad sekretessen faktiskt omfattar, bara själva gatuadressen eller det faktum att personen överhuvudtaget bor i kommunen.

11. Information till den registrerade

Enligt dataskyddsförordningen har den personuppgiftsansvarige informationsplikt gentemot de registrerade. De personer som har sina personuppgifter registrerade ska alltså få information om detta. Information om

personuppgiftsbehandlingen ska lämnas både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

11.1 Information som ska lämnas om personuppgifterna samlas in från den registrerade:

• identitet och kontaktuppgifter till den personuppgiftsansvarige

• dataskyddsombudet

• ändamålet med behandlingen

• den rättsliga grunden.

• om berättigade intressen, vilka dessa är

• mottagarna av personuppgifterna

• laglig grund för överföring till 3:e land (privacy shield, samtycke m.m.)

• den period under vilken personuppgifterna kommer att lagras.

• rätten till rättelse, radering och portabilitet.

• Rätten att återkalla ett samtycke (om behandlingen grundar sig på ett samtycke)

• rätten att klaga till Datainspektionen

• Om personuppgifterna är obligatoriska pga. ett ingånget avtal

• Om profilering förekommer, logiken bakom och följderna av denna

• Information innan personuppgifterna används för annat ändamål

11.2 Information som ska lämnas om personuppgifterna inte har samlas in från den registrerade:

Utöver information under 12.1 ska information om varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor ska information lämnas:

• inom en månad, eller

• senast när första kontakten tas, eller

• när första utlämnade sker

Informationen behöver inte lämnas om det visar sig vara omöjligt eller skulle medföra om proportionell ansträngning, insamlat med lagstöd eller vid tystnadsplikt.

12. Registrerades rättigheter

Rätten till tillgång handlar om att de registrerade själva ska ha rätt att få ta del av den information om dem som finns sparad hos en organisation. Enligt dataskyddsförordningen kan en person be att få ut ett så kallat registerutdrag, det vill säga en kopia på alla de uppgifter som kommunen har samlat på sig om honom eller henne. En begäran om registerutdrag kan komma in till kommunen när som helst. Det är därför viktigt att ha en klar process för hur det ska gå till när man tar fram information om en registerad och lämnar ut den.

12.1. Innehållet i registerutdraget

Att göra ett registerutdrag handlar om att plocka ut de faktiska uppgifterna, inte bara information om dem, och leverera dem till den registrerade. Utdraget kan levereras i form av utskrifter, textfiler, skärmdumpar eller annat, beroende på vad som passar i det aktuella fallet.

All information ska vara begriplig på så sätt att koder och liknande förklaras eller skrivs ut i klartext. Däremot behöver man inte göra översättningar till andra språk eller förklara vedertagna facktermer.

Att lämna felaktiga uppgifter till en person som begär ut information kan leda till sanktionsavgifter på den högre skalan.

Registerutdraget ska innehålla följande information:

• varför personuppgifterna behandlas (ändamålen)

• vilka kategorier av personuppgifter man har behandlat

• om man har lämnat ut personuppgifterna och i sådana fall till vilka kategorier av mottagare

• hur länge man avser att behandla uppgifterna

• om uppgifterna förs över till tredjeland eller en internationell organisation, i sådana fall vart och vilka skyddsåtgärder som vidtagits med anledning av det

• att individen kan ha rätt att rätta, begränsa eller invända mot behandlingen av dennes personuppgifter samt rätt att radera sina personuppgifter och inge klagomål till tillsynsmyndigheten

• källan som uppgifterna hämtats ifrån (om man inte har samlat in informationen själv)

12.1.1. Utdraget ska lämnas inom en månad

All information om en person ska kunna plockas fram och lämnas ut så snabbt det bara går. Man har enligt dataskyddsförordningen högst en månad (30 dagar) på sig att lämna ut ett registerutdrag när en förfrågan kommit in. Det finns dock möjlighet att förlänga den tiden med ytterligare två månader under vissa omständigheter.

Tänk på att det kan vara svårt att förutse hur många förfrågningar som kommer att komma, och likaså när. Arbetsbelastningen kan plötsligt bli ovanligt hög, om organisationen exempelvis av någon anledning får extra uppmärksamhet riktad mot sig.

12.1.2. Utdraget ska lämnas kostnadsfritt

Ett registerutdrag ska vara kostnadsfritt. Organisationen får alltså inte ta ut en avgift från de registrerade som begär att få ta del av sina egna personuppgifter. Skulle en person återkomma med samma begäran flera gånger på ett sätt som kan uppfattas som oskäligt, kan den personuppgiftsansvarige dock ta ut en administrativ avgift eller vägra att lämna fler utdrag.

12.1.3 Utdraget kan behöva skickas elektroniskt

De registrerade har också rätt att få registerutdraget i digitalt format om begäran skickades in digitalt, exempelvis via en webbportal med en stark autentisering vid inloggningen så att man vet att registerutdraget verkligen når rätt person.

12.1.4. Viktigt att säkerställa mottagarens identitet

Tänk på att det är mycket viktigt att säkerställa mottagarens identitet, särskilt om informationen skickas elektroniskt. En enskild individs personuppgifter ska absolut inte skickas till fel person. Det är också viktigt att den information som

skickas ut bara innehåller uppgifter om just den person som efterfrågar registerutdraget, alltså inga personuppgifter om några andra registrerade personer, i vart fall inte om det kan inverka negativt på dem.

12.1.5. Vårdnadshavare eller förvaltare kan begära ut vissa uppgifter

Det finns en möjlighet för vårdnadshavare och förvaltare/god man att begära registerutdrag. Men det kan bero på vilket slags information det rör sig om och vilket uppdrag den gode mannen har. Om man får en sådan förfrågan måste man som personuppgiftsansvarig vara mycket noga med att kontrollera att de påstådda förhållandena är korrekta och att absolut inte lämna ut någon information som kan vara sekretessbelagd till exempel mellan förälder och tonåring.

12.1.6. Blanda inte ihop registerutdrag med offentlighetsprincipen

Blanda inte ihop skyldigheten enligt dataskyddslagstiftningen att lämna registerutdrag, med skyldigheten enligt offentlighetsprincipen att lämna ut allmänna och offentliga handlingar. En handling behöver inte vara vare sig offentlig eller allmän för att den ska ingå i ett registerutdrag.

12.2. Rätt till rättelse

Den registrerade har rätt att få sina felaktiga personuppgifter rättade och kompletterade.

12.3. Rätt till radering

Den registrerade har rätt att få sina uppgifter borttagna (”rätten att bli bortglömd”) om något av dessa skäl finns:

- Uppgifterna inte längre behövs
- Samtycket är återkallat och det saknas annan rättslig grund
- En intresseavvägning väger till den registrerades fördel
- Uppgifterna har behandlats olagligt
- För att uppfylla en rättslig förpliktelse
- Uppgifterna gäller ett barn enligt artikel 8 i dataskyddsförordningen

12.4. Rätt till begränsning av behandling

Den registrerade ska ha rätt att kräva att behandlingen begränsas om behandlingen är felaktig, olaglig och man motsätter sig radering eller i väntan på beslut om radering.

Den personuppgiftsansvarige ska informera mottagarna till vilken personuppgifterna har lämnats om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett i enlighet med artiklarna 16, 17.1 och 18, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

12.5. Rätt till dataportabilitet

- Den registrerade har rätt att få ut uppgifter som man själv har tillhandhållit om sig själv.
- Dessa ska utlämnas i ett maskinläsbart format
- Kan lämnas ut till en ny leverantör eller till den registrerade själv
- Detta gäller endast uppgifter som har lämnats efter samtycke eller som följd av ett ingånget avtal.

12.6. Rätt att göra invändningar

Den registrerade ska ha rätt att göra invändningar:

• när behandlingen grundar sig på intresseavvägning eller allmänt intresse

• när uppgifterna används för direktmarknadsföring

13. Samtycke till behandling av personuppgifter

Samtycke innebär att den registrerade har gett sitt godkännande till att få sina personuppgifter behandlade. I dataskyddsförordningen är utgångspunkten att personuppgiftsbehandling endast är tillåten när den registrerade har lämnat sitt samtycke, om inte annan rättslig grund för behandling finns. Samtidigt ställs det också krav på att information lämnas till de registrerade (läs mer i avsnittet ovan). Läs mer om rättslig grund i tidigare avsnitt.

Ett samtycke ska vara individuellt, frivilligt och särskilt. Ett samtycke kan därför inte lämnas för någon annans räkning och den registrerade ska också ha möjlighet att själv avgöra om personuppgifterna ska få behandlas. Ett lämnat samtycke gäller också för ett enda ändamål, om de insamlade personuppgifterna ska användas för ett annat ändamål än för vilket de samlades in krävs ett nytt samtycke för det nya ändamålet.

För behandling av uppgifter som hör till särskilda kategorier av personuppgifter ställs det högre krav på att samtycket är uttryckligt, alltså att det är extra tydligt. Ett konkludent samtycke där uppgiftslämnandet i sig utgör ett samtycke är inte godtagbart för registrering av uppgifter som hör till särskilda kategorier av personuppgifter.

Ett avtal får inte vara villkorat av ett samtycke till behandling som inte är nödvändig.

I dataskyddsförordningen ställs det däremot inga krav på att samtycket ska vara skriftligt, men det är en god idé att dokumentera inhämtade samtycken eftersom det är den personuppgiftsansvarige som har bevisbördan i de fall ett samtycke ifrågasätts.

13.1. Återkalla samtycke

I de fall en personuppgiftsbehandling utförs endast med stöd av samtycke från den registrerade ska denna ha rätt att när som helst kunna återkalla samtycket. Ett återkallat samtycke innebär att den personuppgiftsansvarige inte får registrera nya uppgifter om den enskilde. Den personuppgiftsansvarige får däremot fortsätta att behandla redan insamlade personuppgifter men de får inte uppdateras eller ändras, risken att dessa också blir rent av felaktiga är därför stor.

14. E-tjänster och personuppgifter

Alla e-tjänster behandlar i någon utsträckning personuppgifter (namn, adress, telefonnummer osv.). Det innebär att dataskyddsförordningen är tillämplig på behandlingen. Om e-tjänsten även behandlar uppgifter som hör till kategorin känsliga personuppgifter krävs extra säkerhetsåtgärder. Valet av autentiseringsmetod bör utgå från känsligheten hos de personuppgifter som behandlas, mängden uppgifter och de risker som är förknippade med behandlingen (se avsnittet om säkerhetskrav ovan).

Observera att myndigheten är personuppgiftsansvarig för all information som registreras i en e-tjänst, även sådan som registreras av den enskilde själv. Kommer det in något olämpligt eller irrelevant, som information om en tredje

person, ska kommunen se till att informationen tas bort eller redigeras så att den blir avidentifierad eller relevant och harmlös. Tänk dock på arkivreglerna, det går inte att gallra information i allmänna handlingar hur som helst.

14.1. Generellt för alla e-tjänster

14.1.1. Information

I anslutning till e-tjänsten ska det lämnas information till användarna om behandlingen av personuppgifter. Det gäller oavsett om uppgifterna samlas in med eller utan de registrerades samtycke. Informationen ska upplysa om vem som är personuppgiftsansvarig, ändamålen med behandlingen, vilka som är mottagare av uppgifterna, eventuell skyldighet för den enskilde att lämna uppgifter och rätten att ansöka om registerutdrag och få felaktiga uppgifter rättade. Normalt kan informationen lämnas i en särskild ruta eller i ett särskilt fönster på webbplatsen i anslutning till e-tjänsten. Detta gäller även för webbaserade enkäter.

Vårdnadshavares samtycke krävs för att ge barn (<13 år) tillgång till Internet-tjänster.

14.1.2. Allmänna handlingar

Tänk på att inkommande och utgående handlingar i en e-tjänst utgör allmänna handlingar utifrån bestämmelserna i offentlighets- och sekretesslagen. Det innebär att daglig diarieföring ska ske vilket omfattar även inkommande och utgående handlingar i e-tjänster.

14.2. Bedöm hur känsliga uppgifterna är

Enligt dataskyddsförordningen gäller särskilda begränsningar för behandling av vissa kategorier av personuppgifter. Uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen, uppgifter om lagöverträdelser samt uppgifter om enskilds personliga förhållanden (extra skyddsvärda uppgifter) ska också behandlas på samma sätt som uppgifter som hör till särskilda kategorier av personuppgifter.

Särskilda krav som ställs på e-tjänst som behandlar uppgifter som hör till känsliga personuppgifter (inklusive extra skyddsvärda uppgifter):

• Användaren av e-tjänsten måste kunna förvissa sig om att det är den personuppgiftsansvarige (nämnden) som är mottagare av uppgifterna. Detta kan lösas genom att till exempel använda ett signerat servercertifikat och SSL/TLS.

• Personuppgifter måste skyddas så att obehöriga inte kan ta del av dem genom exempelvis kryptering och servercertifikat.

• Det krävs fungerande rutiner för behörighetstilldelning och tydliga riktlinjer för när det är tillåtet för personalen att ta del av personuppgifter, här kan utbildningsinsatser vara nödvändiga.

• Det ska finnas en behandlingshistorik (logg) som löpande registrerar användaridentitet, tidpunkt och vilka personuppgifter som användaren har haft åtkomst till eller bearbetat.

Definitioner

Personuppgift

All slags 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. Tänk på att även initialer och annan typ av krypterad eller kodad information kan vara en personuppgift om man med hjälp av anslutande uppgifter kan förstå vem det rör sig om.

Behandling av personuppgift

I dataskyddsförordningen talar man om att personuppgifter behandlas. I stort sett allting man gör med personuppgifter inkluderas när man pratar om en behandling av personuppgifter. Insamling av personuppgifter är en behandling, likaså registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring är andra exempel. Även utskrift är en behandling, utlämnande är en behandling, publicering på en hemsida är en behandling, arkivering och gallring är behandlingar och så vidare.

Observera att informationen inte behöver vara ordnad i någon slags **registerform** för att dataskyddsförordningen ska gälla. Även enstaka personuppgifter i en löpande text är en behandling av personuppgifter i dataskyddsförordningens mening.

Här följer en del exempel på var i en verksamhet personuppgiftsbehandlingar kan förekomma:

- Kund- och leverantörsregister (kontaktpersoner och enskilda näringsidkare)
- Elektroniska besöksliggare och passersystem
- Filmer, bilder och foton av alla de 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 e- postsystemet
- E-tjänster
- Behörighetsadministration och behandlingshistorik (loggar)
- GISar (Geografiska InformationsSystem - kan vara på individnivå när man kan förstå vem eller vilka de olika positioneringarna kan härledas till)
- Kameraövervakning
- Spontanansökningar, rekryteringsdatabaser, kompetensdatabaser, personlighetstester/profiler
- Intranät och publik hemsida
- Egen registerförteckning - till exempel systemägare och kontaktperson för registerutdrag.
- Växelns IT-system lagrar ofta information om vem (vilken anknytning) som har ringt till vem och när
- System som inte längre används.

Känsliga personuppgifter

I dataskyddsförordningen finns ett generellt förbud att registrera känsliga personuppgifter. Bestämmelsen betyder inte att det är helt förbjudet att registrera känsliga personuppgifter, utan man måste hitta ett undantag i förordningen (artikel 9, punkt 2) för att det ska vara tillåtet.

Det är viktigt att lära sig känna igen en känslig personuppgift, så att man inte registrerar sådana på ett felaktigt sätt. I dataskyddsförordningen finns det uttryckligen listat vissa typer av uppgifter, där kallade "särskilda kategorier av personuppgifter", som anses vara integritetskänsliga. Dessa är:

- 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).

Observera att även uppgifter som indirekt avslöjar känslig information av detta slag inkluderas. Det behöver exempelvis inte vara explicit registrerat vilken religion någon tillhör för att uppgiften ska betraktas som känslig, utan det räcker med att man noterat en specifik matpreferens eller liknande. På samma sätt behövs inte att man angivit en sjukdomsdiagnos för att det ska röra sig om känslig hälsoinformation, utan det räcker med till exempel en ansökan om särskola, ett särskilt parkeringstillstånd eller uppgifter om sjukfrånvaro.

Extra skyddsvärda personuppgifter

Förutom gruppen känsliga personuppgifter, som finns definierad i dataskydds-förordningen, så kan också andra uppgifter anses vara integritetskänsliga och därmed vara extra viktiga att skydda. Detta eftersom dataskyddslagstiftningen kräver att man vidtar säkerhetsåtgärder som är lämpliga i förhållande till risken som behandlingen medför för den registrerade.

Exempel på sådana uppgifter är:

- Personuppgifter som omfattas av sekretess eller tystnadsplikt (eller annan särlagstiftning, exempelvis Patientdatalagen)
- Personnummer
- Uppgifter och personliga och ekonomiska förhållanden (inte lön, men införsel på lönen)
- Bild-, ljud- och videoinspelningar
- Omdömen och värderingar av en person såsom social förmåga, inlärningsförmåga och liknande, provresultat, resultat av personlighetstester och annan information som ligger nära den privata sfären.
- Uppgifter om barn
- Uppgifter om lagöverträdelser

Hanterar man extra skyddsvärda personuppgifter behöver man vidta starkare säkerhetsåtgärder för att skydda dem, än vad man behöver göra om alla personuppgifter är harmlösa. Det finns inget förbud mot att behandla dessa, men de ska hanteras med extra försiktighet till exempel genom kryptering och flerfaktorsautentisering (BankID, sms-kod, inloggningskort eller liknande som identifierar användaren på ett säkert sätt) vid kommunikation via öppna nät. E-post med den här typen av personuppgifter ska krypteras enligt Datainspektionens praxis.

Exempelvis registreras det inom skolan en rad extra skyddsvärda uppgifter om barn, bland annat omdömen. Vidtagna säkerhetsåtgärder för registrering av dessa uppgifter gäller inte bara kommunikationen mellan skolan och elev/vårdnadshavare utan också om läraren de facto loggar in sig via internet för att registrera uppgifterna, exempelvis hemifrån.

Helt eller delvis automatiserad behandling

Dataskyddsförordningen tillämpas på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna är avsedda att ingå i ett register.

Helt automatiserad behandling innebär att personuppgifter registreras direkt i exempelvis ett verksamhetssystem och behandlingen framöver fortsätter att ske digitalt.

Delvis automatiserad behandling innebär att personuppgifter samlas i manuellt, exempelvis genom en enkät, med syftet att senare registrera uppgifterna

digitalt. Detsamma gäller om uppgifter som lagras digitalt skrivs ut på papper eller förmedlas vidare muntligt. Vid delvis automatiserad behandling är det viktigt att ha bra rutiner för förvaring och gallring, risken är annars att samma uppgifter sparas på fler platser än nödvändigt.

Manuella register

Manuell behandling av personuppgifter i register (till exempel ett klassiskt kartotek eller när-arkiv) 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.

Personuppgiftsansvarig

Varje nämnd är personuppgiftsansvarig för de behandlingar av personuppgifter som görs inom nämnden. 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, det vill säga nämnden, även när det gäller skadeståndsanspråk enligt dataskyddsförordningen.

Det är personuppgiftsansvariges skyldighet att vidta tekniska och organisatoriska åtgärder för att säkerställa att all behandling av personuppgifter följer dataskyddsförordningen. Dataskyddsförordningen ställer högre krav på att personuppgiftsansvarig ska kunna bevisa att man följer lagstiftningen genom att ha en förteckning, därför är det också viktigt att anmäla de verksamhetssystem som behandlar personuppgifter till dataskyddsombud.

Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för den personansvariges räkning. Personuppgiftsbiträdet finns alltid utanför den personuppgiftsansvariges organisation. Typiska biträdessituationer 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.

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

Personuppgiftsbiträdet är även skyldig att föra en förteckning över sina personuppgiftsbehandlingar man utför åt sina kunder och vidta lämpliga säkerhetsåtgärder. Personuppgiftsbiträdet kan även komma att bli föremål för tillsyn, administrativa sanktionsavgifter samt bli skadeståndsskyldiga.

Dataskyddsombud

Ombudet ska ha koll på vilken behandling av personuppgifter som sker inom organisationen och vara kontaktpunkt mot Datainspektionen. På så sätt liknar rollen den som personuppgiftsombudet tidigare haft. Men i och med dataskyddsförordningen har ombudet har fått en mer omfattande roll. Som dataskyddsombud ska man vara ett bollplank inom organisationen för frågor som rör behandlingen av personuppgifter, och samtidigt vara en övervakare för

att se till att lagar och regler efterföljs. Detta ställer höga krav på förståelse för verksamheten och för hur personuppgifter behandlas i densamma, men det förutsätter samtidigt en självständighet i förhållande till organisationen.