Antaget av kommunstyrelsen 2018-05-15 § 93
Gäller från: 2018-05-25
Ansvarig: Kanslichef
Revideras Vid behov

Riktlinjer för hantering av personuppgifter i Markaryds kommun

MARKARYDS KOMMUN

Innehåll

Riktlinjer för hantering av personuppgifter i Markaryds kommun

1. Inledning

Inom de kommunala verksamheterna hanteras en mängd personuppgifter. Det kan handla om uppgifter om medarbetare, elever, enskilda som söker bygglov eller ekonomiskt bistånd o.s.v. När personuppgifter hanteras måste denna ske i enlighet med lagstiftningen. I detta dokument ges en allmän information om vad som är viktigt att tänka på när en kommunal förvaltning hanterar personuppgifter utifrån gällande lagstiftning. I de olika avsnitten hänvisas till de arbetsrutiner och mallar, vilka ska användas vid hantering av personuppgifter. För de verksamheter där särskilda regler gäller, såsom hälso- och sjukvård, ankommer det på ansvarig nämnd att upprätta de riktlinjer och rutiner som erfordras utöver vad som redovisas i detta dokument.

Den 25 maj 2018 ersätts personuppgiftslagen (PuL) av en ny dataskyddsförordning (GDPR). GDPR (General Data Protection Regulation) är ett regelverk för behandling av person-uppgifter som har tagits fram av EU. Syftet med lagstiftningen är främst att skydda människors personliga integritet vid behandling av deras personuppgifter och därmed rätten till skydd för privatlivet. Som komplettering till GDPR införs även en nationell dataskyddslag.

Bestämmelserna i GDPR är subsidiära, d.v.s. de gäller inte om de skulle komma i konflikt med annan lagstiftning, som exempelvis tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. GDPR hindrar således inte på något sätt kommunens nämnder och bolag från att lämna ut allmänna handlingar enligt offentlighetsprincipen. Däremot är såväl skollagen som socialtjänstlagen underordnade GDPR.

GDPR:s definition av personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

1.1. Allmänt om GDPR

GDPR ska tillämpas på behandlingen av personuppgifter både inom det offentliga och det privata. T.ex. har alla som har sina personuppgifter registrerade hos en kommun rätt att få information om hur deras personuppgifter behandlas.

En del av nyheterna i GDPR kan sammanfattas med:

* Ökade rättigheter för de registrerade
  - Rätt att få sina uppgifter flyttade – dataportabilitet
  - Information och samtycke ska vara tydligare
  - Den registrerade kan överklaga vissa av personuppgiftsansvarigs beslut i ärenden som rör den registrerades rättigheter
* Ökad ansvarsskyldighet för dem som hanterar personuppgifter
  - En dokumenterad konsekvensbedömning ska ske inför behandling som medför särskilda risker
  - Fler aktiva åtgärder från personuppgiftsansvarig och personuppgiftsbiträden
  - Förteckningsskyldighet läggs på den personuppgiftsansvarige?
* Rapporteringsskyldighet vid incidenter
  - Rapportera till Datainspektionen (Integritetsskyddsmyndigheten) vid personuppgiftsincident (inom 72 h)

*Personuppgiftsombud ersätts med ett Dataskyddsombud
*Sanktionsavgift kan utdömas vid brott mot förordningen
*Den s.k. missbruksregeln försvinner - personuppgifter i löpande text/bild och enkla listor räknas också som personuppgiftsbehandling (tex. Word, Excel, e--mail och chattar)

2. Principer för behandling av personuppgifter

Enligt GDPR ska följande principer gälla vid behandling av personuppgifter:

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. All information och kommunikation i samband med behandlingen av personuppgifter ska vara 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 annat ändamål. Det är dock tillåtet att senare använda uppgifterna för arkivändamål, för historiska forskningsändamål eller statistiska ändamål.

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. Med detta menas att kommunen endast ska använda sig av de personuppgifter som krävs för att uppnå målet med hanteringen. Kan samma mål uppnås genom att använda färre personuppgifter eller mindre känsliga sådana ska så ske.

4. Personuppgifterna ska vara korrekta och om nödvändigt uppdaterade. Den personuppgifts-ansvarige ska med rimliga åtgärder säkerställa att personuppgifter som är ogiltiga eller felaktiga i förhållande till de ändamål för vilka de behandlas, raderas eller rättas utan dröjsmål. Inom vissa områden, som hälso- och sjukvård, finns särskilda regler för hur rättelse

och radering får ske. Den personuppgiftsansvarige ska säkerställa att personuppgifter inte förvaras längre än nödvändigt.

5. Personuppgifter ska förvaras i en form som möjliggör identifiering av den registrerade endast under den tid som är nödvändig för de ändamål för vilka personuppgifterna behandlas. Med detta menas att personuppgifterna inte får sparas längre än vad som behövs utifrån målet med behandlingen. När målet är uppnått ska gallring eller avidentifiering av personuppgifterna alltid övervägas med beaktande av de bevarande- och gallringsregler som gäller för kommunen. Uppgifter får t.ex. 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 utifrån deras innehåll. Uppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Med detta menas att personuppgifter ska skyddas genom tekniska och organisatoriska åtgärder på en nivå som motsvarar uppgifternas skyddsvärde. Är uppgifterna av särskilt skyddsvärd art ska också högre tekniska och organisatoriska krav ställas. Utgångspunkten ska alltid vara att endast behöriga personer ska ges tillgång till skyddsvärd information.

3. Ansvarsfördelning inom kommunens organisation

3.1. Personuppgiftsansvarig

Personuppgiftsansvarig enligt GDPR:
”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; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt”. Det vill säga:
Den som bestämmer över personuppgiftsbehandlingen är personuppgiftsansvarig.
I kommunen är det resp nämnd/styrelse/myndighet.

Varje nämnd är personuppgiftsansvarig för de behandlingar av personuppgifter som görs inom nämnden. Det går alltså inte att delegera själva personuppgiftsansvaret. Ansvaret gentemot tillsynsmyndigheten och de registrerade ligger alltid kvar på den personuppgiftsansvarige, det vill säga nämnden, även när det gäller sanktionsavgifter eller skadeståndsanspråk.

3.2. Förteckning över personuppgiftsbehandlingar

Det är personuppgiftsansvariges skyldighet att vidta tekniska och organisatoriska åtgärder för att säkerställa att all behandling av personuppgifter följer GDPR. GDPR ställer krav på att personuppgiftsansvarig ska kunna bevisa att man följer lagstiftningen genom att ha en förteckning över vilka personuppgiftsbehandlingar som förekommer, därför är det också viktigt att anmäla verksamhetssystem som behandlar personuppgifter till dataskyddsombudet. Förteckningen ger stöd för kontroll över vilka personuppgiftsbehandlingar som utförs i kommunen.
Förteckningen, eller registret, är en total kartläggning av alla behandlingar av personuppgifter som utförs inom respektive nämnd. Det ger en översikt över alla register, system och dokument där personuppgifter förekommer. För system som flera nämnders förvaltningar använder är det systemägaren som ansvarar för registreringen av personuppgiftsbehandlingen.

De personuppgiftsansvariga inom Markaryds kommuns organisation är:

- Kommunstyrelsen
- Socialnämnden
- Utbildnings- och kulturnämnden
- Miljö- och byggnadsnämnden
- Överförmyndaren
- Valnämnden
- Revisorerna

samt Markaryds Industribyggnads AB (koncernen)

3.3. Personuppgiftsansvarets omfattning

- Se till att behandlingen av personuppgifter sker i enlighet med dataskyddsförordningen.
- Bestämma för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska utföras.
- Föra register över behandlingar av personuppgifter.
- Informera de registrerade om personuppgiftsbehandling och om de registrerades rättigheter.
- Se till att de anställda har tillräcklig kunskap om dataskyddsförordningen och lämna instruktioner för hur behandlingar ska ske.
- Genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med GDPR.
- Skriva personuppgiftsavtal med personuppgiftsbiträden.
- Besluta om delegering av arbetsuppgifter som rör behandling av personuppgifter inom den egna verksamheten.
- Utse ett dataskyddsombud och anmäla detta till Integritetsskyddsmyndigheten.

Notera:

- Den personuppgiftsansvarige kan aldrig överlåta sitt ansvar till någon annan. Däremot är det övergripande ansvaret för arbetet med behandling av personuppgifter delegerat till förvaltningschefen. Respektive förvaltningschef kan i sin tur, mot bakgrund av de personuppgiftsansvarigas beslut, vidaredelegera det operativa arbetet till minst en handläggare inom förvaltningen.

- Dataskyddsförordningen kräver en konsekvensbedömning av den personuppgiftsansvarige innan särskilt känsliga behandlingar av personuppgifter genomförs. I detta arbete måste dataskyddsombudet rådfrågas.

Bilaga/länk: Instruktion, inkl mall, för registeranmälan om personuppgiftsbehandling

3.4. Dataskyddsombud

Ett dataskyddsombud är en person som ser till att personuppgifter behandlas på ett korrekt och lagligt sätt inom organisationen. Dataskyddsombudet kan jämföras med en internrevisor som påpekar fel och brister till den som är personuppgiftsansvarig. När varje personuppgiftsansvarig myndighet (nämnd/styrelse) utsett ett dataskyddsombud anmäls det till Integritetsskyddsmyndigheten (tidigare Datainspektionen) på särskild blankett. Uppsägning av dataskyddsombud ska också anmälas till Integritetsskyddsmyndigheten

I dataskyddsombudets uppdrag ingår bland annat att självständigt och oberoende se till att den personuppgiftsansvariga behandlar personuppgifter på ett lagligt och korrekt sätt. Eventuella brister påpekas för den personuppgiftsansvarige. Förslag till åtgärder lämnas på samma gång. I det fall den personuppgiftsansvarige inte vidtar några åtgärder för att komma till rätta med de brister som påtalats, ska dataskyddsombudet anmäla detta till Integritetsskyddsmyndigheten.

Dataskyddsombudet har också en rådgivande funktion och ska informera, ge råd och stöd till både personuppgiftsansvariga, förvaltningschef, handläggare och allmänheten. Det förutsätts att dataskyddsombudet har en självständig och oberoende ställning i förhållande till de personuppgiftsansvariga och förvaltningarna/bolagen. Dataskyddsombudet får ha andra arbetsuppgifter också, men dessa får inte leda till en intressekonflikt för ombudet.

Dataskyddsombudet ska kontinuerligt rapportera direkt till respektive förvaltningschef och påpeka eventuella brister. Självklart är ombudet bunden till sekretess och tystnadsplikt. Dataskyddsombudets kontaktuppgifter ska offentliggöras så att ombudet är lättillgängligt för kommunens registrerade personer. Dataskyddsombudet ska vara sammankallande för kommunkoncernens nätverk för arbetet med GDPR med tillhörande lagar och regler. Markaryds kommun har tecknat avtal med kommunalförbundet Sydarkivera om anlitande av personal vid Sydarkivera till uppdraget som dataskyddsombud.

3.5. Handläggare för personuppgiftsbehandlingar

Respektive personuppgiftsansvarig (nämnd/styrelse) delegerar det övergripande ansvaret för arbetet med behandling av personuppgifter till förvaltningschefen som i sin tur kan vidare-delegera det operativa arbetet till minst en handläggare inom förvaltningen. Handläggaren har en operativ roll och ska samråda med samt får råd och stöd av kommunens dataskydds-ombud i sitt arbete. Vidare lämnar handläggaren nödvändiga uppgifter/underlag till dataskyddsombudet och ingår i kommunens nätverk för arbetet med GDPR.

3.6. Delegering av beslutanderätt

Till den/de som utses till handläggare av personuppgiftsfrågor inom resp nämnds förvaltning, bör även delegeras rätten att fatta beslut i de ärenden om personuppgiftshantering där nämnden, enligt GDPR, kan bifalla eller avslå en ansökan/begäran från den registrerade. Med sådana beslut avses ärenden där den registrerade ansöker eller begär tillgång till personuppgifter enligt bestämmelserna i GDPR artikel 15-21. Om kommunen avslår en sådan begäran ska kommunen kunna visa att begäran är uppenbart orimlig eller ogrundad. Den registrerade kan överklaga beslutet till allmän förvaltningsdomstol. Kommunen är skyldig att informera om möjligheten att överklaga då beslutet meddelas.

3.7. Personuppgiftsbiträde

Personuppgiftsbiträde enligt GDPR: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgifts-ansvariges 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 person-uppgifter, utan gäller även när en extern part har åtkomst till den personuppgiftsansvariges data genom sitt uppdrag för service, support, underhåll, utveckling och liknande.

Enligt GDPR får endast personuppgiftsbiträden förekomma som ger tillräckliga garantier om att skyldigheterna i förordningen kommer att uppfyllas och att de registrerades rättigheter skyddas. GDPR kräver att ett biträdesavtal upprättas mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Det är alltid systemägaren som svarar för att personuppgiftsbiträdesavtal (PUB-avtal) tecknas. Vid upphandlingar av leverantörer som ska agera personuppgiftsbiträden åt kommunen måste det ställas krav på att vinnande leverantör ingår personuppgiftsbiträdesavtal som uppfyller GDPR:s krav. PUB-avtal som upprättats innan 25 maj 2018 ska uppdateras.

I ett flertal situationer kommer även personuppgiftsbiträden att omfattas av samma skyldigheter som gäller för personuppgiftsansvariga. Detta gäller bland annat skyldighet att föra register över behandlingar, utse dataskyddsombud, samarbete med tillsyns-myndigheten (Integritetsskyddsmyndigheten), ansvar för att vidta säkerhetsåtgärder, att omgående underrätta den personuppgiftsansvarige om personuppgiftsincidenter, att bistå den personuppgiftsansvarige. Personuppgiftsbiträdet kan även komma att bli föremål för tillsyn, administrativa sanktionsavgifter samt bli skadeståndsskyldiga.
Bilaga/länk: Mall för personuppgiftsbiträdesavtal

4. När är det tillåtet att behandla personuppgifter?

4.1. Nödvändighet

För alla behandlingar av personuppgifter finns alltid ett krav på nödvändighet. De personuppgifter som samlas in ska vara nödvändiga för ändamålet och därför ska heller inga onödiga personuppgifter samlas in. Det bör därför återkommande ifrågasättas om alla de uppgifter som registreras faktiskt är nödvändiga för ändamålet. Det är sällan ett person-nummer behövs på en deltagarlista till exempel.

Alla personuppgiftsbehandlingar måste ha en rättslig grund, till exempel avtal (anställningsavtal, avtal med kund), allmänt intresse (forskning, statistik, arkiv) myndighetsutövning (bygglov, ekonomiskt bistånd) och rättsliga förpliktelser (till exempel bokföringsskyldighet). Kommunens behandling av personuppgifter omfattas för det mesta av något av sådana ändamål. Detta innebär att samtycke endast behöver användas i undantagsfall, då det inte finns någon rättslig grund för personuppgiftsbehandlingen. Om samtycke ska användas måste det finnas en fri valmöjlighet för den registrerade. Enbart samtycke bör undvikas, eftersom det när som helst kan återkallas och då får man inte behandla personuppgiften längre om man inte kan åberopa en annan grund för behandlingen.

4.2. Inget krav på samtycke

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.
- **Vitala intressen** - Behandling av personuppgifter är tillåten om det sker för att skydda den registrerades vitala intressen som liv och hälsa. Exempel: Vanligt inom sjukvården (patientdatalagen).
- **Allmänt intresse** - Gäller när behandling av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse. För att en arbetsuppgift ska vara av allmänt

intresse ska den regleras i svensk lagstiftning eller lagstiftningen inom EU. Det betyder att de aktuella personuppgifterna måste behandlas för att utföra ett uppdrag som är reglerat i lagstiftning eller som det är fattat beslut om. En särskild lag behöver dock inte pekas ut för varje enskild behandling, utan det kan räcka med en lag som grund för flera behandlingar. Kommunens nämnder är myndigheter där större delen av verksamheterna regleras i lag eller kommunala beslut, därför är verksamheten i huvudsak av allmänt intresse.

- **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. Detta är också en vanlig grund för personuppgiftsbehandlingar inom inom kommunen. 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. (Det krävs f.ö. inga samtycken inom socialtjänstlagens område.)
- **Eget offentliggörande** - När den registrerade själv uppger sina personuppgifter. Till exempel de förtroendevaldas partitillhörighet.
- **Intresseavvägning** - Kan tillämpas när den personuppgiftsansvariges intresse att behandla en uppgift väger tyngre än den enskildes personliga integritet, när ändamålet för behandlingen rör ett berättigat intresse hos den personuppgiftsansvarige.
  OBS! En intresseavvägning bedöms inte vara tillåten för myndigheter/kommuner i den nya dataskyddsförordningen (GDPR). Undantaget från många personuppgiftsregler vid ostrukturerad behandling – den så kallade missbruksregeln – kommer att försvinna. Vanliga exempel på ostrukturerad behandling av personuppgifter är i e-post och på hemsidor där personuppgifter hanteras i löpande text.

4.3. Känsliga personuppgifter

I GDPR benämns känsliga personuppgifter som ”särskilda kategorier av personuppgifter”. Uppgifter som gäller särskilda kategorier av personuppgifter är i regel förbjudna att behandlas. Det måste finnas en bestämmelse om undantag i GDPR (artikel 9) som medger behandling av sådana uppgifter. Definitionen av särskild personuppgift i GDPR motsvarar, med vissa ändringar, personuppgiftslagens benämning känsliga personuppgifter och omfattar uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt genetiska och biometriska uppgifter med vilka man entydigt kan identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Vid behandling av sådana uppgifter ska en konsekvensbedömning göras (se nedan).

Vad gäller uppgifter om t.ex. kontonummer, uppgift om försäkringsskydd, utbetalningar av ersättningar, uppgifter om kontohavanden m.m. utgör dessa inte känsliga personuppgifter

enligt GDPR. Datainspektionen har däremot uttalat att denna typ av uppgifter ska betraktas som känsliga personuppgifter vid fastställande av vilka lämpliga skyddsåtgärder den personuppgiftsansvarige ska vidta för att skydda de behandlade uppgifterna.

4.4. Extra skyddsvärda personuppgifter

Datainspektionen har gjort en distinktion mellan särskilda/känsliga personuppgifter och andra personuppgifter som man anser vara extra skyddsvärda (kan även kallas integritetskänsliga) men som inte omfattas av definitionen om särskilda/känsliga personuppgifter. Exempel på sådana uppgifter är:

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

Det finns inget förbud mot att behandla dessa uppgifter, men de ska hanteras med extra försiktighet. GDPR kräver att säkerhetsåtgärder vidtas som tar hänsyn till uppgifternas art och den risk som behandlingen innebär för den registrerade. Konsekvensbedömning ska göras (se nedan). Datainspektionen har även ställt krav på att starka säkerhetsåtgärder vidtas för det fall att sådana extra skyddsvärda personuppgifter på något sätt registreras så att de finns att nå via internet (öppna nät), exempelvis efter inloggning.

4.5. Samtycke

Personuppgifter får behandlas om man har ett samtycke från den som personuppgifterna avser. Samtycket ska vara:

- Frivilligt
- Skriftligt, med tydligt angivet ändamål med behandlingen
- Lämnas innan behandlingen påbörjas och efter det att den registrerade har fått information om dataskyddsförordningen tillsammans med den personuppgiftsbehandling som samtycket gäller för.

Den som behandlar personuppgifter med stöd av samtycke måste kunna vissa att ett giltigt samtycke har lämnats av den registrerade. Den registrerade ska få tillräcklig information om behandlingen för att förstå innebörden av samtycket. 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. Särskilt höga krav gäller när samtycke avser behandling av känsliga uppgifter. En anhörig kan inte lämna sitt samtycke för exempelvis en dement person, samtycke kan i vissa fall lämnas av en förvaltare och i vissa fall av en god man. Samtycket ska vara tidsbegränsat.

4.6. Barns samtycke

I den nya dataskyddslagen anges att barn som fyllt 13 år på egen hand ska kunna samtycka till behandling av personuppgifter när de använder sociala medier och andra informationstjänster.

4.7. Återkalla samtycke

Samtycke får alltid återkallas. Ett återkallat samtycke innebär att den personuppgiftsansvarige inte får registrera nya uppgifter om den enskilde om personuppgiftsbehandlingen sker enbart med stöd av samtycke. Den personuppgiftsansvarige får däremot fortsätta att behandla redan insamlade personuppgifter men de får inte uppdateras eller ändras.

Bilaga/länk: Mall för samtycke

5. Säkerhetskrav vid personuppgiftsbehandling

5.1. Åtgärder

Den personuppgiftsansvariga nämnden/bolaget är skyldig att vidta sådana säkerhetsåtgärder som skyddar de personuppgifter som behandlas. Åtgärderna ska vara så utformade att de ger en relevant säkerhetsnivå med hänsyn till tekniska möjligheter, kostnader, särskilda risker med behandlingen av personuppgifterna och hur känsliga de behandlande uppgifterna är. Datainspektionen (Integritetsskyddsmyndigheten) får i enskilda fall besluta om vilka säkerhetsåtgärder som den personuppgiftsansvariga ska vidta.

Tekniska åtgärder omfattar saker som brandväggar, krypteringsfunktioner och anti-virus, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation, rutiner och styrdokument. 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.

5.2. Personuppgiftsincident

En säkerhetsincident definieras vara något som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörig röjande eller obehörig åtkomst till de personuppgifter som överfört, lagrats eller på annat sätt behandlats.

Exempel: diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust brott mot sekretess eller tystnadsplikt. En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har blivit förstörda, gått förlorade på annat sätt, kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

Exempel på incidenter:

- Någon har kommit över ett lösenord som gör det möjligt att logga in i system som behandlar personuppgifter.
- Ett mail med känsligt eller extra skyddsvärda personuppgifter skickas till fel mottagare.
- Ett glömt papper i skrivare som innehåller uppgifter om namn och sjukdomstillstånd.
- En dator har fått skadlig kod som gör att obehörig skulle kunna komma åt personuppgifter.

En personuppgiftsincident ska anmälas av den personuppgiftsansvarige till Datainspektionen (Integritetsskyddsmyndigheten) inom 72 timmar efter att den har upptäckts. Detta gäller även om incidenten inträffat hos ett av kommunens biträden, det vill säga någon av kommunens leverantörer. Därför är det viktigt att varje medarbetare rapporterar inträffad personuppgiftsincident. Någon anmälan behöver dock inte göras om det är osannolikt att incidenten leder till några risker för enskildas fri- och rättigheter. Om en personuppgiftsincident däremot bedöms sannolikt kunna leda till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige också informera de registrerade om säkerhetsincidenten. I GDPR föreskrivs närmare om vad informationen till de registrerade ska innehålla.

Alla personuppgiftsincidenter ska rapporteras. Det är viktigt för att kommunen ska kunna agera vid både allvarliga och mindre allvarliga brister. Varje medarbetare ansvarar för att rapportera om risk för, misstanke om eller inträffande av en personuppgiftsincident.

Bilaga/länk: Mall för incidentrapportering/anmälan

5.3. Konsekvensbedömning

Vid personuppgiftsbehandlingar som sannolikt medför en hög risk för den registrerades integritet måste en konsekvensbedömning genomföras. En konsekvensbedömning beskriver syftet med personuppgiftsbehandlingen samt risker som kan uppstå för den vars personuppgifter behandlas.

Syfte med bedömningen är

- att förebygga risker innan de uppkommer
- att bedöma om personuppgifterna som samlas in är nödvändiga för ändamålet
- att bedöma om den personuppgiftsansvarige har vidtagit tillräckliga åtgärder för att skydda den registrerades integritet och rättigheter.

En konsekvensbedömning som medför hög risk för den registrerades integritet ska genomföras

- innan en ny personuppgiftsbehandling påbörjas
- vid pågående behandlingar som inte konsekvensbedömts tidigare, eller
- vid pågående behandlingar där risken ändrats (ökat).

I GDPR har den personuppgiftsansvarige en skyldighet att genomföra en konsekvensbedömning, en typ av risk- och sårbarhetsanalys, för varje ny behandling av känsliga personuppgifter. Konsekvensbedömningen är ett effektivt hjälpmedel för den personuppgiftsansvarige att säkerställa en korrekt och säker behandling av personuppgifter. Resultatet från konsekvensbedömningen ska dokumenteras.

Att genomföra en konsekvensbedömning för en särskild personuppgiftsbehandling är en bra utgångspunkt för att säkerställa en säker och korrekt behandling. I konsekvens-bedömningen 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.

Bilaga/länk: Mall för konsekvensbedömning

5.4. Särskilt om 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: sekretessmarkering, kvarskrivning och fingerade personuppgifter.
När det gäller behandling av skyddade personuppgifter ska den personuppgiftsansvarige, utöver att se till att behandlingen följer GDPR, 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.

6. Den registrerades rättigheter

6.1. Allmän översikt

6.1.1. Rätt till information

Alla personer har rätt att veta hur deras personuppgifter hanteras inom kommunen. Det gäller oavsett hur uppgifterna har kommit kommunen till del. (Se vidare nedan)

6.1.2. Registerutdrag

Enskilda personer har rätt att få bekräftelse på om och hur deras personuppgifter hanteras inom kommunen och även få tillgång till dem om så är fallet. Var och en har också rätt att begära ut ett registerutdrag som innehåller de personuppgifter som behandlar denne. (Se vidare nedan)

6.1.3. Rätt till rättelse

Alla personuppgifter som behandlas inom kommunen ska vara korrekta och rimligt aktuella för ändamålet. Annars ska de rättas. Alla enskilda har rätt att begära att en felaktig uppgift rättas. Om uppgifter rättas på den enskildes begäran måste företaget eller myndigheten också informera dem som de har lämnat ut uppgifter till om att uppgifter rättats. Det gäller dock inte om det skulle visa sig omöjligt eller innebär en alltför betungande insats. Den enskilde har också rätt att begära att få information om till vem uppgifter har lämnats ut.

6.1.4. Rätt till radering

Enskilda personer har under vissa förutsättningar rätt att få sina personuppgifter raderade. För att rätt till radering ska aktualiseras krävs att något av följande är uppfyllt:

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

Det finns undantag från rätten till radering och skyldigheten att informera andra om det är nödvändigt för att tillgodose andra viktiga rättigheter som till exempel rätten till yttrande- och informationsfrihet, för att uppfylla en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Kommunen kan således avslå en begäran om radering med hänvisning till dessa skäl. Den enskilde kan då klaga över beslutet hos Integritets-skyddsmyndigheten.
Markaryds kommun och dess nämnder är enligt arkivlagen och av kommunfullmäktige antaget arkivreglemente skyldiga att arkivera och gallra allmänna handlingar. Det finns ett för resp nämnd regelverk för vilka handlingar som ska bevaras och gallras samt eventuella gallringsfrister (dokumenthanteringsplaner). Som offentligrättsligt organ torde det inom Markaryds kommun endast i undantagsfall bli aktuellt med tillämpning av bestämmelserna om radering.

6.1.5. Rätt till begränsning av användning

Enskilda har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Med begränsning menas att uppgifterna markeras så att dessa i framtiden endast får behandlas för vissa avgränsade syften.
Om någon registrerad påpekar ett fel ska dennes rätt till begränsning respekteras under tiden föreningen eller förbundet utreder.

6.1.6. Dataportabilitet

Den som har lämnat sina personuppgifter har i vissa fall rätt att få ut och använda sina personuppgifter på annat håll till exempel i en annan social medietjänst (rätten till dataportabilitet). Den som har tagit emot personuppgifterna är skyldig att underlätta en sådan överflyttning av personuppgifter. En förutsättning är att denna behandlar personuppgifterna med stöd av ett samtycke från den registrerade eller för att uppfylla ett avtal med den registrerade och det gäller bara sådana personuppgifter som den registrerade själv har lämnat. Rätten till dataportabilitet är en nyhet i dataskyddsförordningen. I nuläget görs bedömningen att begäran om dataportabilitet inte kommer att bli aktuell i någon vidare utsträckning inom kommunen.

6.1.7. Rätt att göra invändningar

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

Om den enskilde invänder mot behandlingen i sådana fall får den personuppgiftsansvarige endast fortsätta att behandla uppgifterna om det går att visa att det finns tvingande berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den enskildes intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk. Den enskilde har alltid rätt att invända mot att hans eller hennes personuppgifter används för direkt marknadsföring. En sådan invändning kan göras när som helst. Görs en invändning mot direkt marknadsföring, får personuppgifterna inte längre behandlas för sådana ändamål.

6.1.8. Rätt att inte bli föremål för automatiserat beslutsfattande

Den enskilde har rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande, inbegripet profilering, om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne.

Automatiserat beslutsfattande kan till exempel vara ett automatiserat avslag på en kreditansökan på internet eller vid ett nekande besked från e-rekrytering via internet utan personlig kontakt.
Automatiserat beslutsfattande kan vara tillåtet om det är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige eller om den enskilde har gett sitt uttryckliga samtycke. Det kan även vara tillåtet enligt särskild lagstiftning.

6.1.9. Klagomål

Kommunen (den personuppgiftsansvarige) ska upplysa den registrerade att om denne inte är nöjd med hur kommunen hanterar dennes personuppgifter kan den registrerade vända sig till tillsynsmyndigheten för att lämna klagomål. Datainspektionen, som är tillsynsmyndighet, kommer under 2018 att byta namn till Integritetsskyddsmyndigheten.
Exempel – information som alltid ska ges:
”Om du inte är nöjd med hur dina personuppgifter behandlats eller upplever att dina uppgifter blivit felaktigt hanterade har du möjlighet att lämna klagomål hos tillsynsmyndigheten (Integritetsskyddsmyndigheten”). Rätten att lämna klagomål ska inte förväxlas med rätten att överklaga ett beslut där kommunen avslår en begäran från den registrerade att vidta en åtgärd med anledning av bestämmelserna om den registrerades rättigheter.

6.2. Kommunens informationsplikt mot registrerade personer

6.2.1. Allmänt

Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige 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.
Om personuppgifter som rör en registrerad person samlas in ska följande information lämnas;

- Identitet och kontaktuppgifter för den ansvariga nämnden
- Ändamålen med behandlingen
- Den rättsliga grunden för behandlingen
- Information om personuppgifterna kan komma att lämnas ut till tredje part och i så fall för vilka syften
- Rätten att begära registerutdrag
- Rätten att få sina personuppgifter rättade vid felaktigheter eller raderade
- Hur länge personuppgifterna kommer att lagras

Bilaga/länk: Mall/exempel på informationstext

6.2.2. Information som ska lämnas självmant

Den personuppgiftsansvarige ska alltid lämna information om en behandling av personuppgifter till den registrerade innan behandlingen påbörjas. Inhämtas personuppgifterna från den registrerade, lämnas informationen i samband med insamlandet. Inhämtas personuppgifterna från någon annan än den registrerade själv, ska den personuppgiftsansvarige lämna informationen i samband med att personuppgifterna registreras första gången.

6.2.3. Undantag

Information behöver inte lämnas om uppgifterna inhämtas från någon annan och den registrerade redan känner till informationen eller om det visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats att lämna information.
Information ska inte heller lämnas om personuppgifterna måste fortsätta vara konfidentiella till följd av att vissa uppgifter omfattas av sekretess.

6.2.4. Informationens omfattning

Beroende på om den personuppgiftsansvarige samlar in personuppgifter direkt från den registrerade eller om den personuppgiftsansvarige har fått uppgifterna från någon annan än den registrerade finns det vissa olikheter i informationens omfattning. Gemensam information rör den personuppgiftsansvarige, kontaktperson/er, dataskyddsombudet, uppgifter om ändamålet med personuppgiftsbehandlingen i fråga, den information som behövs för att den registrerade ska kunna ta tillvara på sina rättigheter i samband med behandlingen såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgift och rätten att ansöka om information och få rättelse. (Se mall/exempel på informationstext.)

6.2.5. Den enskildes rätt till registerutdrag

Var och en har rätt att vända sig till kommunen och begära att få veta vad som finns registrerat om dennes personuppgifter. Varje personuppgiftsansvarig, d.v.s. varje nämnd, ska då kontrollera om det föreligger någon personuppgiftsbehandling av den här personen i sin verksamhet. Om så är fallet ska skriftlig information ges om:

- Ändamålet med behandlingen
- Vilka uppgifter om den sökande som behandlas (t.ex. namn och personnummer)
- Varifrån uppgifterna hämtas (från den registrerade själv eller från annan källa)
- Till vilka mottagare uppgifterna lämnas ut (Lämnas uppgifter till vårdgivare eller annan myndighet t.ex.)
- Eventuell överföring till tredje land och i så fall vilka skyddsåtgärder har vidtagits
- Hur länge verksamheten sparar handlingarna (kontrollera dokumenthanteringsplan)
- Rätten att lämna klagomål till Integritetskyddsmyndigheten
- Förekomsten av automatiserat beslutsfattande och vilka följderna blir för den registrerade
- Rätten att bli raderad (om det inte står i strid med offentlighetsprincipen)
- Rätten att kunna invända mot och begränsning av personuppgiftsbehandlingen

Den sökande kan bara få information om behandling av sina egna personuppgifter. Föräldrar till minderåriga kan få ta del av uppgifter om sina barn. Det är den personuppgiftsansvarige som ansvarar för att registerutdraget är korrekt och lämnas i tid och det görs under straffansvar. Registerutdraget ska lämnas ut inom en månad. Det finns dock möjlighet att vänta upp till tre månader innan utdraget lämnas, men då ska det föreligga särskilda skäl och den som begär utdraget ska informeras om förseningen och orsaken till den. Det ska då vara sakliga skäl för förseningen. Som sakliga skäl räknas inte semester, arbetsanhopning eller att det råder osäkerhet om var personuppgifterna kan finnas registrerade någonstans.

Rätten till information avser inte utlämnande av uppgifter om en registrerad, utan att tillgodose en informationsskyldighet mot registrerade. Därutöver kan den registrerade begära tillgång till sina uppgifter, närmare bestämt en kopia av sina uppgifter. Skyldigheten att lämna registerutdrag enligt GDPR har således inget att göra 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. Registerutdragen som lämnas blir däremot alltid allmänna handlingar, som kan vara offentliga eller omfattas av sekretess enligt de vanliga reglerna om offentlighet och sekretess.

6.2.6. Säkerställ att registerutdraget skickas till rätt person och inom rätt tid

I den nya dataskyddsförordningen är det möjligt att begära ett registerutdrag skriftligt eller elektroniskt och då ska det även vara möjligt att få den informationen i ett elektroniskt format. Om sökande vill ha kopiorna i pappersform ska de skickas med rekommenderat brev. Lämna inte ut ett registerutdrag om en begäran kommit in per e-post eller muntligen, om det inte är säkerställt att utlämning görs till rätt person. Skicka alltid registerutdrag till folkbokföringsadress och innehåller registerutdraget känsliga personuppgifter så bör försändelsen dessutom skickas som rekommenderat brev.

Registerutdraget behöver inte innehålla personuppgifter från löpande text som inte fått sin slutgiltiga utformning (arbetsmaterial) när den registrerade gjorde sin ansökan eller personuppgifter från minnesanteckningar. Detta eftersom personuppgifterna inte är sökbara och Integritetsskyddsmyndigheten menar att det inte heller skulle gagna den enskildes integritet att göra identitetsuppgifter i sådant material sökbara. Vid osäkerhet om hur en begäran om registerutdrag ska hanteras ska förvaltningens handläggare för personuppgiftsärenden och ev. dataskyddsombudet tillfrågas.

Om uppgifter om den sökande inte behandlas i kommunkoncernens register, ska information om detta meddelas per post eller e-post inom en månad från det att ansökan inkom till kommunen.

Bilaga/länk: Arbetsrutin inkl mall för registerutdrag

7. Publicering av personuppgifter på internet

7.1.1. Allmänt

Personuppgifter om enskilda får endast publiceras på hemsidan om det finns rättslig grund för det. Det måste beaktas att personuppgifter som enskilt kan betraktas som harmlösa kan anses som kränkande beroende på sammanhanget de publiceras i. Känsliga eller extra skyddsvärda personuppgifter får aldrig publiceras på webben. Obs! Känsliga 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.

7.1.2. Samtycke är ett möjligt alternativ för att godkänna publicering

Om det råder osäkerhet om en uppgift kan anses vara integritetskränkande kan möjligheten att hämta in samtycke användas. Samtycker den enskilde så kan uppgifterna publiceras . Fyller den enskilde i en ansökan digitalt eller i pappersformat så kan samtycke inhämtas i samband med ansökan. Viktigt är att alla samtycken, dokumenteras för att kunna hänvisa till dessa.

7.1.3. Personuppgifter på internet

Det är generellt förbjudet att överföra personuppgifter till länd utanför EU eller EES-området (tredje land). Det är ändå tillåtet om den registrerade har lämnat sitt samtycke till överföringen eller om överföringen är nödvändig för att uppnå vissa, i lagen, specificerade områden. Någon överföring av uppgifter till tredje land föreligger inte när personuppgifter läggs ut på internet och den som tillhandahåller servertjänsten är etablerad i ett EU-land. OBS! Personnummer får aldrig publiceras på någon av kommunkoncernens hemsidor. Publicering av personuppgifter på kommunkoncernens hemsidor måste ske med försiktighet. Publiceringen får aldrig vara förolämpande, ärekränkande eller liknande.

7.1.4. Publicering av foton m.m.

Harmlösa personuppgifter som namn, befattning, telefonnummer och e-post till arbetet och liknande arbetsrelaterade personuppgifter, kan normalt publiceras på en webbplats utan den registrerades samtycke – om publiceringen är berättigad och inte innebär en kränkning av den personliga integriteten. 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 (exempelvis porträttfoton i kombination med namn och eventuella kontaktuppgifter). Undantaget gäller bland annat hemtjänstpersonal, fastighetsskötare eller liknande för att kunden ska veta att den släpper in rätt person i sitt hem. Även personer i ledande ställning, som tjänstemannaledningen, får räkna med att få sin bild publicerad på hemsidan.

Personuppgifter som rör en förtroendevald och hans/hennes uppdrag får publiceras. Till exempel namn och partitillhörighet.
Personuppgifter om familjeförhållanden, bostadsadress, telefonnummer och fritidsintressen är normalt inte harmlösa uppgifter och ska absolut inte publiceras. Foton på anställda kräver samtycke från den anställde.

För att säkerställa den personliga integriteten bör samtycke alltid lämnas då personer kan identifieras på fotot – oavsett sammanhang. Om någon invänder mot att personuppgifter om henne/honom har publicerats på internet, bör uppgifterna tas bort även om de kan verka harmlösa för utomstående.

7.1.5. Publicering av uppgifter om skolelever

Uppgifter om elevers namn, skol- och klasstillhörighet, liksom e-postadress i skolan får publiceras på hemsidan. Inom skola, förskola och fritids måste vårdnadshavare samtycka innan en publicering på hemsidan av personuppgifter om barn som rör hemadress, hemtelefonnummer, eget mobilnummer, foton med mera. Samtycket ska inhämtas från båda vårdnadshavarna.
OBS! Personuppgifter om elever med skyddad adress får aldrig publiceras.

8. Särskilt om sociala medier

När Markaryds kommun som organisation publicerar personuppgifter i sociala medier (Facebook, Twitter, Instagram, Youtube m.fl.) ingår i personuppgiftsansvaret att:

- inte publicera kränkande personuppgifter,
- hålla regelbunden uppsikt över publiceringar för att upptäcka kränkande personuppgifter,
- skyndsamt ta bort kränkande personuppgifter,
- vidta lämpliga säkerhetsåtgärder (det innebär bland annat att kommunen ska ge instruktioner till dem som arbetar med sociala medier på uppdrag av kommunen).

I personuppgiftsansvaret ingår det 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 tillsynsmyndigheten 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.

Bilaga/länk till kommunens riktlinjer för sociala medier

9. Personuppgiftsbehandling - riktlinjer kring e-post

Hantering av personuppgifter i e-post räknas också som behandling av personuppgifter och samma krav gäller som för alla andra behandlingar. Det krävs i GDPR en laglig grund för behandling av personuppgifter i e-post.

En stor del av den personuppgiftsbehandling som förekommer i en kommunal myndighets e-post kan hänföras till den lagliga grunden ”arbetsuppgifter av allmänt intresse” (art. 6.1 e) såvida innehållet eller ämnet berör de arbetsuppgifter myndigheten har att fullgöra inom ramen för den kommunala kompetensen, t.ex. e-post i bygglovsärenden med invånare. Även den lagliga grunden ”rättslig skyldighet” kan läggas till grund för behandling av personuppgifter i sådan e-post, t.ex. enligt dokumentationskrav i förvaltningslagen eller annan speciallagstiftning. administrativa funktioner och åtgärder i den kommunala förvaltningen (prop. 2017/18:105 s. 61), t.ex. e-post till och från kontaktpersoner hos leverantörer eller liknande. Med stöd av den lagliga grunden uppgifter av allmänt intresse kan myndighet behandla personuppgifter inom den frivilliga verksamheten, om behandlingen är nödvändig, t.ex. e-post inom kultur- och idrottsförvaltningen(prop. 2017/18:105 s. 56). Likaså för dagliga administrativa funktioner och åtgärder i den kommunala förvaltningen (prop. 2017/18:105 s. 61), t.ex. e-post.

GDPR påverkar kommunens e-posthantering och kräver att en översyn görs av arbetssätt och rutiner kring hantering av personuppgifter i e-post. Som grundregel kan sägas att hantering av personuppgifter ska främst ske i system, inte i e-post.

Ett e-postmeddelandet med personuppgifter bör inte ligga kvar i inkorgen eller i skickat-mappen under längre tid. När behandlingen av personuppgifter är klar bör informationen flyttas över till lämpligt system och/eller raderas från e-postsystemet. Den tid som en personuppgift lagras i e-posten ska begränsas till ett strikt minimum. Bestämmelserna om allmänna handlingar enligt offentlighets- och sekretesslagen och arkivlagen har dock alltid företräde. Radering av personuppgifter i e-post som utgör allmänna handlingar får därför endast ske enligt gällande dokumenthanteringsplan.

I e-posten får inte personuppgifter som är känsliga eller sekretessbelagda behandlas eller sparas. Om känsliga eller sekretessbelagda personuppgifter inkommer kan man till exempel inte vidarebefordra eller svara på e-postmeddelandet om inte särskilda säkerhetsåtgärder kan göras för att undanröja risken för att personuppgifterna sprids på felaktigt sätt.

Känsliga eller extra skyddsvärda personuppgifter ska inte skickas via e-post, till exempel uppgifter om någons hälsa, religiösa åskådning eller politiska åsikter. Undvik även att skicka andra integritetskänsliga uppgifter som exempelvis värderingar av en person, provresultat eller andra uppgifter. Använd e-post för att kommunicera, inte för att lagra.

Bilaga/länk E-postpolicy.

10. Hantering av personnummer

I den nya dataskyddslagen 3 kap 10-11 §§ anges:
”10 § Personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.
11 § Regeringen får meddela ytterligare föreskrifter om i vilka fall behandling av personnummer och samordningsnummer är tillåten.”

Det finns inget 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. Personnummer får behandlas utan samtycke bara när det är absolut nödvändigt.
Personnummer ska inte användas i e-post, på hemsida eller i sociala medier.
Även om registrering av personnummer är tillåten bör personnummer inte skrivas ut på listor, förteckningar med mera. Personnummer får endast skrivas ut om det är klart motiverat. Födelsedatum räknas inte som personnummer och kan skrivas ut på förteckningar. Till exempel klasslistor - om personuppgiftsbehandlingen i övrigt är tillåten.
Överväg alltid om det är nödvändigt att notera personnummer. Det är framförallt den slentrianmässiga användningen av personnummer som man måste vara observant på, exempelvis i mejlkonversationer. Beakta därför om syftet med behandlingen av personuppgifter kan anses berättiga att personnummer registreras?

Personnummer ska enbart användas:

- om den registrerade har samtyckt till registreringen,
- om behandling är klart motiverat med hänsyn till ändamålet med behandlingen (räcker det med förslagsvis namn och adress, födelsedatum eller födelseår)
- om behandling 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 ovan nämnda 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.
- om behandling är klart motiverat med hänsyn till något annat beaktansvärt skäl.

Bestämmelserna om personnummer gäller inte födelsedatum. Datainspektionen har ändå ansett att det är tveksamt om det finns anledning att registrera födelsedatum på till exempel en deltagarlista.

11. Ta bort personuppgifter

11.1. Allmänt

Det är ändamålet, alltså anledningen till att personuppgifterna behandlas, som normalt avgör hur länge uppgifterna får sparas innan de gallras. 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 företräde framför bestämmelserna i GDPR.

11.2. Hur tar man bort personuppgifter?

Det finns två olika sätt att ta bort personuppgifter. Man kan antingen avidentifiera eller förstöra (gallra) dem. Ingen allmän handling får förstöras utan att det finns ett beslut om att gallring ska ske.

12. Särskilt om personuppgifter i e-tjänster

12.1. Allmänt

Alla e-tjänster behandlar i någon utsträckning personuppgifter (namn, adress, telefonnummer osv.). Det innebär att GDPR är tillämplig på behandlingen. Om e-tjänsten även behandlar 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.

12.2. 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.

12.3. Personuppgiftsbiträdesavtal

Om en utomstående leverantör av e-tjänsten behandlar personuppgifter för nämndens räkning, till exempel om de lagras på en server hos leverantören, blir denne ett personuppgiftsbiträde.

13. Rättsmedel

13.1. Skadestånd och sanktionsavgifter

Ansvaret för behandling av personuppgifter ligger på den personuppgiftsansvariga nämnden. Datainspektionen (Integritetsskyddsmyndigheten) är tillsynsmyndighet över tillämpningen av GDPR och utdömer skadestånd och/eller sanktioner om det råder brister i tillämpningen och/eller de registrerades personuppgifter behandlas i strid mot GDPR och den kompletterande datalagen.

Den personuppgiftsansvarige ska ersätta den registrerade för skada och kränkning av den personliga integriteten om detta orsakats av olaglig behandling av hans/hennes personuppgifter.

13.2. Sanktionsavgift

I Dataskyddslagen 6 kap anförs:
”2 § Tillsynsmyndigheten får ta ut en sanktionsavgift av en myndighet vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i EU:s dataskyddsförordning, i den ursprungliga lydelsen. Då ska artikel 83.1, 83.2 och 83.3 i förordningen tillämpas. Sanktionsavgiften ska bestämmas till högst 5 000 000 kronor vid överträdelser som avses i artikel 83.4 i EU:s dataskyddsförordning och till högst 10 000 000 kronor vid överträdelser som avses i artikel 83.5 och 83.6 i förordningen.
3 § Tillsynsmyndigheten får ta ut en sanktionsavgift vid överträdelser av artikel 10 i EU:s dataskyddsförordning, i den ursprungliga lydelsen. Då ska artikel 83.1, 83.2 och 83.3 i förordningen tillämpas. Avgiftens storlek ska bestämmas med tillämpning av artikel 83.5 i förordningen.”

Ytterligare information finns på Integritetsskyddsmyndighetens hemsida www.datainspektionen.se.