Plan
Policy
Handlingsplan
Riktlinje

Uppdaterad 2018-07-02

Så hanterar vi personuppgifter

Enligt Dataskyddsförordningen (GDPR)

Forshaga kommun

Fastställt av: Kommunens ledningsgrupp

Fastställt datum: 2018-12-11

Dokumentet gäller till och med: Tills vidare

Dokumentet gäller för: Alla nämnder och förvaltningar

Dokumentansvarig: Kommunledningskontoret

Diarienummer: KS 2018/401

Vision och budget med strategisk plan Vision: ***"Forshaga barnkommun**. I våra barn finns framtiden och vi bygger ett samhälle för nuvarande och kommande generationer. Genom hållbara, långsiktiga och ansvarstagande lösningar får vi en attraktiv och trygg kommun även i framtiden."*
Kommunfullmäktiges budget med strategisk plan är kommunens viktigaste övergripande styrdokument. I budgeten återfinns också vår vision, det önskvärda framtida tillståndet för kommunen och kvalitets- och styrmodellen som övergripande beskriver hur den kommunala verksamheten ska styras, följas upp och utvärderas. Strategisk plan innehåller kommunens övergripande mål, värdegrund och tre hållbarhetsstrategier.

Plan anger inriktning och konkreta mål i en fråga av större vikt. Den är vägledande för beslut och styrning. Planen tar inte ställning till utförande eller metod. Har en begränsad giltighetstid och ska följas upp. Exempel på plan kan vara Bostadsförsörjningsplan. Beslutas av kommunfullmäktige, kommunstyrelsen eller nämnd.

Policy är ett kortfattat dokument på en övergripande nivå om specifika, strategiskt viktiga områden. Den är vägledande för beslut och styrning. Policy tar inte ställning till utförande eller metod. En policy är vanligtvis långvarig, och gäller tills vidare. En policy bör konkretiseras i andra styrdokument, oftast i riktlinjer. Exempel på policy kan vara Upphandlingspolicy och Kommunikationspolicy. Beslutas av kommunfullmäktige, kommunstyrelsen eller nämnd.

Handlingsplan är en sammanställning av aktiviteter som tillsammans ska leda till att uppnå mål. Den visar konkret vad som ska göras inom ett visst område, vem/vilka som ansvarar för uppgiften, ekonomiska konsekvenser samt när det ska vara klart alternativt när det ska följas upp. Omsätter ofta inriktningen i planen till konkreta åtgärder. Exempel på handlingsplan kan vara Handlingsplan för nybyggnation av flerfamiljshus på Åsmyren. Beslutas av kommunchef, förvaltningschef eller ledningsgruppen.

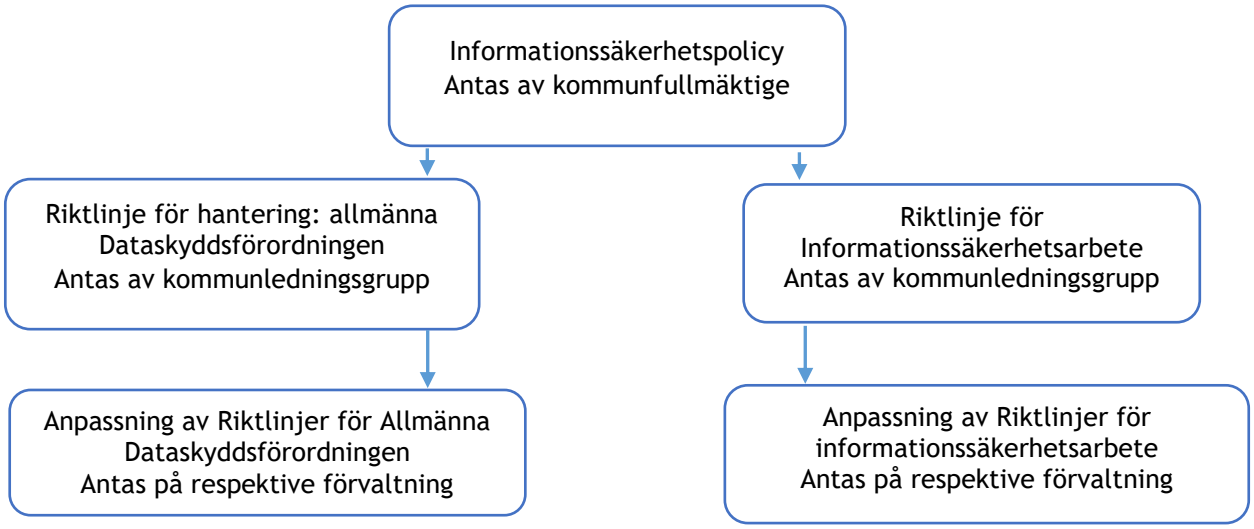
Riktlinjer är den mest konkreta formen av styrdokument. Ett dokument som innehåller en anvisning eller rekommendation för hur exempelvis en policy ska uppnås. Riktlinjer avser främst frågor rörande ren verkställighet. Riktlinjer kan betraktas som en slags handbok som ska ange ramarna för vårt handlingsutrymme i en viss fråga. Gäller tillsvidare vilket innebär att gamla riktlinjer måste upphävas när de blir inaktuella. Exempel på riktlinjer kan vara Riktlinjer för användande av sociala medier. Beslutas av kommunchef, förvaltningschef eller ledningsgruppen.

Innehåll

Riktlinjeför hantering: Allmänna Dataskyddsförordningen (GDPR)

1. Inledning

Denna riktlinje utgör Forshaga kommuns övergripande styrdokument för att hantera och implementera Dataskyddsförordningen (GDPR)[1], och för att säkerställa att kommunens anställda lever upp till de krav som förordningen ställer.
Alla verksamheter där kommunen har ett huvudmannaansvar är bundna av denna riktlinje, vilket medför att det inte finns utrymme att besluta om lokala avvikande regler.
Forshaga kommuns arbete med Informationssäkerhet i allmänhet och Allmänna Dataskyddsförordningen i synnerhet kan beskrivas enligt följande modell:



2. Syfte och mål

Syftet med denna riktlinje är att ange hur Forshaga kommun säkerställer att de krav och villkor som anges i Allmänna Dataskyddsförordningen uppfylls. Målet med denna riktlinje är att alla verksamheter där kommunen har ett huvudmannaansvar ska förstå hur de ska implementera Allmänna Dataskyddsförordningen i sin specifika verksamhet.

2.1 Avgränsning

I denna riktlinje avser gentemot sådant som faller utanför Allmänna Dataskyddsförordningens lagrum.

3. Vad innebär GDPR för kommunen?

Från och med den 25 maj 2018 gäller Allmänna Dataskyddsförordningen (nedan kallad GDPR). Efter engelskans General Data Protection Regulation, ersätter bland annat Personuppgiftslagen[2] och innebär i korthet att kommunen måste föra register över sin behandling av personuppgifter, samt att alla incidenter som berör personuppgifter måste anmälas till tillsynsmyndigheten[3]. Förordningen

[1] EU:s förordning nr 2016/679
[2] Personuppgiftslagen (PUL) 1998:204
[3] Datainspektionen

innebär också att konsekvensbedömningar måste göras innan nya behandlingar av personuppgifter sker. Nytt är också de höga sanktionsavgifter som kan utdömas.

3.1 Allmänt säkerhetskrav för kommunen

I enlighet med GDPR[4] ska Forshaga kommun och dess anställda utforma sina IT-system, sin IT-användning och sina rutiner enligt principen om inbyggt dataskydd och dataskydd som standard (privacy by design samt privacy by default). Det allmänna säkerhetskravet ska också efterlevas då IT-system/rutiner är i drift, och kommunen som helhet ska ständigt sträva efter att förbättra sitt säkerhetsskydd, både tekniskt och organisatoriskt.

3.2 Viktiga definitioner[5]

Forshaga kommuns definitioner följer GDPR.

Behandling: en åtgärd eller kombination av åtgärder som rör personuppgifter eller uppsättningar av personuppgifter, exempelvis insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Ostrukturerad behandling: Behandling av personuppgifter i listor, minnesanteckningar, löptext, bild och ljud, likställs numera med övriga personuppgifter, och är således inte tillåtna utan laglig grund[6]

Personuppgifter: all slags information som avser en fysik person (nedan kallad ”den registrerade” eller ”den enskilde”) som är identifierad eller kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsansvarig: en offentlig myndighet eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Också ansvarig för behandlingen av personuppgifter. *Nämnder i Forshaga kommun är personuppgiftsansvariga*.

Personuppgiftsbiträde: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Personuppgiftsincident: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Profilering: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Pseudonymisering: anonymisering av personuppgifter/behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används. Krypterade uppgifter som går att tolka eller av kryptera räknas alltså *inte* som pseudonymiserade.

---

[4] artikel 25
[5] artikel 4
[6] se avsnitt 9.4.2

Register: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

Skyddsåtgärder, organisatoriska: Åtgärder som syftar till att skydda personuppgifterna genom att anställda har kunskap om lagstiftningen samt att verksamheten som helhet är uppbyggd för att säkerställa skyddet av personuppgifter. Exempelvis regelbunden utbildning, antagna styrdokument, tydliga rutiner, och en vision om att ständigt förbättra sitt säkerhetsskydd.

Skyddsåtgärder, tekniska: Åtgärder som syftar till att skydda personuppgifterna genom säker teknik som är byggd för att hantera och säkerställa de krav GDPR anger. Exempelvis säkra IT-system, kryptering och behörighetskontroll, samt lämpliga uppdateringar.

Tredje part: en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna.

4. Ansvarsfördelning och roller

Personuppgiftsansvarig (nämnden) har yttersta ansvar för att säkerställa att behandling av personuppgifter inom den egna nämnden sker i enlighet med lagstiftningen och kommunens styrdokument. Det är också personuppgiftsansvarig som ansvarar för att meddela tillsynsmyndigheten vid personuppgiftsincident[7], samt att vid tillsyn kunna redovisa hur de säkerställer Dataskyddsförordningens krav och villkor[8]. *Det är dock i första hand kommunens anställda som var och en måste ansvara för att Dataskyddsförordningen och kommunens styrdokument efterlevs inom det dagliga arbetet.*

4.1 Förvaltningsspecifika riktlinjer för hantering

Varje förvaltning upprättar vid behov förvaltningsspecifika riktlinjer/hänvisningar för hantering av personuppgifter enligt GDPR, där den praktiska implementeringen av GDPR beskrivs. På så sätt visar Forshaga kommun hur lagens krav och villkor uppfylls och säkerställs utifrån varje förvaltnings specifika förutsättningar.

4.2 Förvaltningsspecifika informationsägare

Samtliga nämnder ska utse minst en informationsägare som säkerställer att Dataskyddsförordningen, liksom kommunens styrdokument, efterlevs på förvaltningen. Förvaltningens informationsägare har som främsta uppgift att agera rådgivande och stöttande gentemot förvaltningens anställda i deras arbete med Dataskyddsförordningen. Informationssäkerhetssamordnaren har alltså en skyldighet att

a) Hålla sig uppdaterad om lagstiftningen och praxis
b) Säkerställa att anställda inom förvaltningen får den utbildning de behöver för att leva upp till Dataskyddsförordningens krav
c) Säkerställa att förvaltningens behandling av personuppgifter registreras i kommunens registerföringssystem, samt att förvaltningens registerförda behandling av personuppgifter lever upp till lagstiftningen
d) Säkerställa att förvaltningens Riktlinjer för hantering av personuppgifter hålls aktuell och relevant
e) Kunna svara på frågor från anställda inom förvaltningen, kommunens dataskyddombud, samt tillsynsmyndigheten, gällande förvaltningens arbete med Dataskyddsförordningen

[7] Artikel 33
[8] Artikel 56

f) Se till så att rutiner för anmälan av personuppgiftincidenter till tillsynsmyndigheten finns
g) Agera stöd då konsekvensbedömningar behöver göras vid ny behandling av personuppgifter.

4.3 Kommunens Dataskyddsombud

Enligt Dataskyddsförordningens[9] är Forshaga kommunens nämnder skyldiga att utse ett dataskyddombud.

Dataskyddsombudets uppgifter är att agera rådgivande åt kommunens nämnder, att hjälpa till vid konsekvensbedömningar, att på ett övergripande plan övervaka efterlevnaden av Dataskyddsförordningen, samt att vara kontaktperson mot tillsynsmyndigheten[10].
Dataskyddsombudet utgör också en rådgivande och stöttande instans gentemot nämndernas informationsägare.

5. Personuppgifter

Forshaga kommuns behandling av personuppgifter ska alltid ske i enlighet med de principer[11] som tas upp i Dataskyddsförordningen. Vidare får Forshaga kommuns faktiska behandling av personuppgifter enbart ske då minst ett av de lagstadgade skälen uppfylls[12].
Personer vars personuppgifter blir behandlade av Forshaga kommun ska alltid få information om var personuppgifterna finns lagrade, vilka personuppgifter det gäller, hur personuppgifterna lagras, samt vem den registrerade kan kontakta för frågor gällande behandling av Personuppgifter[13].
Informationen ska förmedlas på ett lättförståeligt sätt.[14]. Den registrerade ska också få information om vilka rättigheter den enskilde har gentemot kommunen. I tillämpliga fall ska den registrerade även meddelas om vilken tidsperiod personuppgifterna kommer lagras. Information om Forshaga kommuns behandling av personuppgifter ska också finnas på kommunens hemsida. För praktisk tillämpning av ovan skall-krav, hänvisas till respektive förvaltnings riktlinjer/hänvisningar för hantering av personuppgifter enligt Dataskyddsförordningen.

5.1 Allmänna principer för behandling av personuppgifter

Forshaga kommun följer de principer som Dataskyddsförordningen anger för behandling av personuppgifter[15]. Principerna utgör ett grundkrav för kommunens behandling av personuppgifter, och ska alltid följas. Det är personuppgiftsansvariga som har ansvar för att principerna följs[16].

- **Laglighet, korrekthet och öppenhet.** Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.
- **Ändamålsbegränsning.** Uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. De insamlade personuppgifterna får behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål utan att det anses oförenligt med de ursprungliga ändamålen om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.
- **Uppgiftsminimering.** Uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

---

[9] artikel 37
[10] Artikel 39
[11] artikel 5 punkt1
[12] Artikel 6
[13] Artikel 13 och 14
[14] Artikel 12 punkt1
[15] Artikel 5
[16] Artikel 5 punkt 2

- **Korrekthet.** Uppgifterna ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.
- **Integritet och konfidentialitet.** Uppgifterna får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. De insamlade personuppgifterna får lagras under längre tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.
- **Ansvarsskyldighet.** Uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

5.2 Skäl för behandling av personuppgifter

Forshaga kommun kräver att minst ett av nedanstående skäl[17] föreligger för att personuppgifter ska få behandlas. Det är upp till personuppgiftsansvarig att kunna bevisa att giltigt skäl föreligger.

a) **Samtycke.** Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål. *Obs, kan i princip inte användas av kommun på grund av ojämnt maktförhållande.* Får enbart användas för komplettering där annat lagligt skäl redan finns - exempelvis för att publicera en bild på medborgare, medarbetare eller förtroendevalda på någon av kommunens websidor. Samtycket ska vara skriftligt, och kunna dras tillbaka närsomhelst.
b) **Avtal med den registrerade.** Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
c) **Rättslig förpliktelse**. Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Alltså: annan laglig grund krävs för behandling. Även kollektivavtal, domar (praxis) och tyngre myndighetsbeslut räknas in i detta skäl.
d) **Skydda grundläggande intressen.** Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
e) **Uppgift av allmänt intresse eller myndighetsutövning.** Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning – det vill säga: legal grund i form av tydliga, precisa och förutsägbara regler, exempelvis kommunala reglementen och registerförfattningar.
f) **Intresseavvägning.** Behandlingen är nödvändig för ändamål som rör personuppgiftsansvariges berättigade intressen. *Obs, intresseavvägning får inte användas för att motivera behandlingar inom offentlig organ (kommunen).*

5.2.1 Skäl för hantering av särskilt känsliga personuppgifter

Känsliga personuppgifter är sådana uppgifter som avslöjar information som kan vara till skada för den registrerade – med andra ord, ”värderade uppgifter”.

Känsliga uppgifter utgörs av personuppgifter som **avslöjar ras/etniskt ursprung, politisk åsikt, religiös/filosofisk övertygelse, medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter, uppgifter om hälsa samt uppgifter om en fysisk persons sexualliv eller sexuella**

[17] Artikel 6

läggning[18]. Även så kallade integritetskänsliga uppgifter (exempelvis personnummer eller uppgifter om brott) samt ***alla personuppgifter som rör barn faller under denna kategori***.

Känsliga/integritetskänsliga personuppgifter får dock behandlas om någon av följande skäl föreligger (Artikel 9 punkt 2):

a) Särskilt samtycke. *Kan ej användas av kommunen*
b) **Arbetsrätt med mera.** Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt nationell rätt och gällande kollektivavtal.
c) **Skydda grundläggande intressen.** Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
d) **Berättigad behandling av stiftelse/förening.** *Kan ej användas av kommunen*
e) Personuppgifter är redan kända. Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
f) **Nödvändigt för rättsförfarande.** *Kan ej användas av kommunen*
g) **Viktigt allmänt intresse.** Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av nationell rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
h) **Krävs för hälso- och sjukvård.** Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg med yrkesverksamma på hälsoområdet som innehar tystnadsplikt. Notera att användning enligt Socialtjänstlagen inte faller under denna punkt, då detta faller under punkt e Myndighetsutövning i de ordinarie skälen.
i) **Krävs för att upprätthålla folkhälsa.** Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, där de behandlande innehar tystnadsplikt.
j) **Krävs för särskilda arkivändamål, forskningsändamål eller statistiska ändamål.** Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med nationell rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Utgångspunkten är att all behandling av uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden[19].

5.3 Utlämnande av personuppgifter

Nämnden eller av nämnden utsedd tjänsteman ska alltid säkerställa att om ifall personuppgifter måste lämnas ut, ska detta göras med hänsyn till personuppgifternas art och känslighet. Nämnden ska hellre vara för restriktiva med utlämnade, än för generösa. Det enda undantaget

[18] Artikel 9
[19] Artikel 9 punkt 1

gäller när registrerad begär ut personuppgifter om sig själv. I övrigt gäller att personuppgifter enbart får lämnas ut om de inte strider mot Offentlighets- och sekretesslagen, vilken klargör att utlämnande av personuppgifter aldrig får äventyra den enskildas säkerhet och rätt till integritet. Även Dataskyddsförordningen klargör att personuppgifter ska sekretessmarkeras snarare än lämnas ut[20], om inte uttryckligt samtycke getts[21]. Skulle nämnden ha svårt att avgöra huruvida den begärande parten har rätt till vissa personuppgifter, kan nämnden avböja att lämna ut så länge den begärande parten inte kan identifiera sig mer precist[22]. För överföring mellan myndigheter gäller att principerna för behandling av personuppgifter uppfylls, samt att den registrerade får tydlig information om syfte, vilka personuppgifter det gäller och när uppgifterna överförs[23]. Vid till syner eller liknande visning av personuppgifter måste en anställd från Forshaga kommun närvara då tredje part tar del av personuppgifterna. Då känsliga uppgifter visas ska ett sekretessavtal skrivas under.

5.3.1 Begäran om fullständigt registerutdrag

Den registrerade har alltid rätt att begära ut personuppgifter om sig själv eller den som personen är vårdnadshavare för[24]. Denna information ska lämnas ut skyndsamt, men senast efter 30 dagar[25] .

Den registrerade har rätt att begära ett kostnadsfritt registerutdrag per år. Vill den registrerade begära ut fler registerutdrag per år, kommer en avgift att tas ut[26]. Registrerad ska kunna styrka sin identitet vid begäran om registerutdrag.
Följande information ska finnas med i registerutdraget för varje behandling som registrerad finns med i:

- Syftet med behandlingen
- De kategorier av personuppgifter som behandlas
- De mottagare/kategorier av mottagare som personuppgifterna har lämnats ut till
- Från vem personuppgifterna i behandlingen inhämtas ifrån
- (Om möjligt) Under vilken period personuppgifterna kommer lagras i behandlingen
- Om det förekommer automatiserat beslutsfattande
- Den enskildas rättigheter

5.4 Konsekvensbedömning vid personuppgiftsbehandling

Om någon av kommunens personuppgiftsansvariga planerar en ny eller omfattande förändring i behandling av personuppgifter som innebär hög risk för de registrerade, ska denna föregås av en konsekvensbedömning[27]. Konsekvensbedömningen ska syfta till att vara förutseende, förebygga risker och därmed skydda människors fri- och rättigheter. Konsekvensbedömningen ska göras innan personuppgiftsbehandlingen påbörjas, eller om riskerna med en pågående behandling har ändrats.
Hög risk definieras i Forshaga kommun som att

a) En stor mängd personuppgifter behandlas, och då särskilt om dessa är känsliga personuppgifter
b) Många olika typer av personuppgifter behandlas, och då särskilt om dessa är känsliga personuppgifter
c) Flera olika personer har tillgång till personuppgifterna

---

[20] Artikel 86
[21] Artikel 20 punkt 1
[22] Artikel 11 punkt2
[23] Artikel 13-14 och Artikel 20
[24] Artikel 15
[25] Artikel 12 punkt 3 och 4
[26] Artikel 15 punkt 3
[27] Artikel 35

d) Personuppgifterna berörs av delvis eller helt automatiserad behandling (exempelvis systematisk kamera/övervakning, samkörning av register eller bakgrundsgranskning)
e) Personuppgifterna rör personer som av något skäl befinner sig i underläge eller beroendeställning
f) Personuppgifterna ska behandlas med hjälp av helt ny teknik
Samtliga konsekvensbedömningar i Forshaga kommun ska klargöra hur många uppgifter som samlas in, vilken rättslig grund det finns för insamlandet, samt för vilket ändamål uppgifterna får behandlas. Konsekvensbedömningarna ska också ta reda på de risker som finns för behandlingen, samt hur dessa risker ska bemötas. Det är upp till varje personuppgiftsansvarig att genomföra relevant konsekvensbedömning. Konsekvensbedömningen ska sparas tillsammans med registerföringen av det personuppgiftsbehandlande systemet, samt uppdateras vid behov.

5.5 Säkerhet vid behandling av personuppgifter

Utöver kommunens allmänna säkerhetskrav att följa principen om inbyggt dataskydd och dataskydd som standard, ska kommunens anställda beakta särskild försiktighet när det kommer till behandlingen av personuppgifter[28]. Det är personuppgiftsansvarig som har det yttersta ansvaret för att lämpliga tekniska och organisatoriska åtgärder vidtas för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med att behandla personuppgifterna. De säkerhetsåtgärder som kan vara lämpliga utgörs exempelvis av men är ej begränsat till:

a) pseudonymisering och kryptering av personuppgifter
b) rutiner för att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingsystemen och – tjänsterna (klassificering av informationshanteringssystemen)
c) rutiner för att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet
e) en konsekvent uppdaterat och fungerande behörighetskontroll så att varje anställd, personuppgiftsbiträde eller extern mottagare enbart får tillgång till den information som berör aktuellt ärende
f) avrådan mot att använda fritextfält i personuppgiftshanterande system till att skriva beskrivande/personliga reflektioner, om detta inte är absolut nödvändigt och kan motiveras av Dataskyddsförordningen

5.5.1 Den enskildes rättigheter

Forshaga kommun ska säkerställa att den enskildes rättigheter såsom fastställs i Dataskyddsförordningens[29]uppfylls. Detta är en viktig säkerhetsåtgärd, och den praktiska implementeringen av rättigheterna förtydligas i respektive nämnds *Riktlinjer för hantering av Dataskyddsförordningen*. Rättigheterna är som följer:

- **Rätt till information:** Den registrerade har rätt att få information när hens personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det, samt vid exempelvis personuppgiftsincidenter eller när ändring har skett enligt någon av nedanstående punkter.
- **Rätt till rättelse:** Varje registrerad person har rätt att vända sig till kommunen och be att få uppgifter kompletterade eller felaktiga uppgifter rättade.

[28] artikel 32
[29] Artikel 15-22

- **Rätt till radering (rätten att bli bortglömd)[30]:** gäller inte vid *rättslig förpliktelse, myndighetsutövning eller allmänt intresse*.
- **Rätt till begränsning av behandling**: Enskild 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, och inom kommun gäller detta enbart att registrerad kan motsätta sig att personuppgifter raderas (exempelvis för att enskild vill använda dem i bevisändamål) eller om mycket specifika skäl föreligger vid exempelvis utredningar.
- **Dataportabilitet:** *Obs, gäller enbart vid vissa avtal med elektroniskt lagrade uppgifter*. Den som har lämnat sina personuppgifter har i vissa fall rätt att få ut och använda sina personuppgifter på annat håll, och den som har tagit emot personuppgifterna är då skyldig att underlätta en sådan överflyttning av personuppgifter.
- **Rätt att göra invändningar:** *Gäller enbart när laglig grunden är Allmänt intresse*. En enskild har i vissa fall rätt att invända mot den personuppgiftsansvariges behandling av hens personuppgifter. Följden kan bli att uppgifter raderas eller begränsas.
- **Automatiserat beslutsfattande, inbegripet profilering:** Den enskilde har rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande som innefattar profilering, om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar den enskilde. Undantag kan gälla om det exempelvis är nödvändigt för att fullgöra ett avtal.

  Utöver dessa punkter har den enskilde också rätt att lämna klagomål på kommunens behandling av den enskildes personuppgifter, men detta görs till tillsynsmyndigheten[31]. Skulle tillsynsmyndigheten finna att kommunen eller kommunens personuppgiftsbiträde brustit i sin efterlevnad av Dataskyddsförordningen, kan den enskilde begära skadestånd av kommunen eller dess biträde i domstol[32].

5.6 Anmälan om personuppgiftsincident till tillsynsmyndigheten

Om det inträffar en säkerhetsincident som rör personuppgifter (exempelvis dataintrång eller oavsiktlig förlust av personuppgifter) ska denna incident dokumenteras och anmälas till tillsynsmyndigheten inom 72 timmar[33]. Personuppgiftsincidenterna innefattar förlust (personuppgifterna förstörs eller går ej längre att komma åt), förstöring (personuppgifterna har ändrats, blivit korrumperade eller inte längre är kompletta) eller obehörigt röjande/åtkomst (personuppgifterna har avslöjats till mottagare som inte är behörig, eller på annat sätt får åtkomst). Även om en fullständig anmälan inte kan göras, ska det som kan dokumenteras skickas in till tillsynsmyndigheten inom 72 timmar. Det är personuppgiftsansvarig, alternativt anlitade personuppgiftsbiträden, som har ansvar för att göra anmälan för incidenter inom sina respektive Nämnder[34].
Hur incidenter upptäcks, dokumenteras och anmäls till tillsynsmyndigheten definieras i nämndernas Riktlinjer för hantering av Dataskyddsförordningen. Anmälan behöver dock inte göras om det är osannolikt att incidenten leder till några risker för de registrerades fri- och rättigheter, exempelvis vid kortare tillgänglighetsincidenter. Forshaga kommun rekommenderar dock sina anställda att anmäla, snarare än att inte anmäla. Samtliga incidentanmälningar ska innehålla (lättförståelig) information om:

[30] Artikel 17 punkt 2b
[31] Artikel 77 och 78
[32] Artikel 82
[33] Artikel 33
[34] Artikel 33 punkt 1 och 2

- Vilken typ av incident det är frågan om
- Vilka kategorier av personer som kan komma att beröras
- Hur många personer det berör
- Vilka konsekvenser incidenten kan få
- Vilka åtgärder nämnden vidtagit för att motverka eventuella negativa konsekvenser
- Kontaktuppgifter till personuppgiftsansvariges informationssäkerhetssamordnare, eller annan där mer information om incidenten kan fås

Personuppgiftsansvariga och deras anlitade personuppgiftsbiträden har också en skyldighet att informera den/de registrerade som drabbas av incidenten[35]. Detta ska ske utan dröjsmål och innehålla den information som även skickats med anmälan till tillsynsmyndigheten. Den registrerade ska också få råd om hur hen kan skydda sig mot ytterligare skada, utifrån den specifika incident som skett.

6. Registerföring över behandling

Både kommunens personuppgiftsansvariga och kommunens anlitade personuppgiftsbiträden är skyldiga att föra ett register över sin behandling av personuppgifter[36]. Forshaga kommun har ett kommungemensamt registerföringssystem för att hantera registren över behandling av personuppgifter, men det är varje personuppgiftsansvarigs ansvar att föra in vilka register över behandling som de innehar inom sin nämnd.

Nämnderna är med andra ord skyldiga att hålla nämndens registerförda behandlingar uppdaterade och korrekta.

På begäran ska den personuppgiftsansvarige dessutom kunna göra registret tillgängligt för tillsynsmyndigheten. Hur dessa tillsynsbesök ska hanteras får varje nämnd avgöra själva. Forshaga kommuns program för registerföringen ska innehålla följande uppgifter för varje enskild registerförd behandling:

a) Namn och kontaktuppgifter för den personuppgiftsansvarige, den personuppgiftsansvariges företrädare samt dataskyddsombudet
b) Ändamålen/syftet med behandlingen
c) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter
d) De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer
e) Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter
f) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som används för att skydda uppgifterna

7. Kommungemensamma behandlingar av personuppgifter

Forshaga kommun delar tre verksamheter med grannkommuner. Dessa tre verksamheter utgörs av Överförmyndarnämnden (vilken Forshaga kommun är värdkommun), samverkansnämnden (IT-avdelning vilken Kils kommun är värdkommun) och miljö och bygg nämnden (Forshaga kommun är värdkommun). För att säkerställa att personuppgifter hanteras på ett korrekt sätt av de kommunerna inom samtliga tre verksamheter, ska personuppgiftsbiträdesavtal upprättas mellan kommunernas kommunstyrelser.

Personuppgiftsbiträdesavtalet ska beskriva hur biträdeskommunen förvaltar det system som personuppgiftsansvarig kommun tillhandahåller, och hur personuppgifter i det gemensamma systemet behandlas på ett säkert och lagligt sätt även av biträdeskommunen. I övrigt gäller att

[35] Artikel 34
[36] Artikel 30

samtliga kommungemensamma verksamheter följer detta styrdokument samt Dataskyddsförordningen i sin helhet.

8. Personuppgiftsbiträden

Vid anlitande av personuppgiftsbiträde ska alltid ett skriftligt personuppgiftsbiträdesavtal tecknas[37]. Avtalet ska klargöra att personuppgiftsbiträdet och dess personal enbart får behandla personuppgifter **enligt instruktion** från den personuppgiftsansvarige[38], samt att biträdet inte får anlita andra biträden utan att ha fått ett skriftligt tillstånd av den personuppgiftsansvarige[39]. De biträden som kommunen anlitar ska dessutom kunna ge tillräckliga garantier för att deras behandling uppfyller kraven i Dataskyddsförordningen[40]. Detta innebär exempelvis att biträdet ska registerföra sin behandling av personuppgifter, samt att biträdet vid tillsyn ska kunna redovisa att de tillhandahåller en lämplig säkerhetsnivå för sin hantering av känslig information[41].

I avtal som Forshaga kommun upprättar ska personuppgiftsbiträdet åta sig att:

- Bara behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige
- Se till så att personer som har behörighet att behandla personuppgifter hos biträdet har åtagit sig att iaktta tystnadsplikt eller omfattas av lagstadgad sådan
- Vidta alla tekniska och organisatoriska åtgärder som är nödvändiga för att säkerställa en lämplig säkerhetsnivå i förhållande till riskerna med behandlingen
- Respektera kraven på förhandstillstånd och avtal vid anlitande av ett annat biträde (exempelvis underbiträden). Kunna redovisa kontaktuppgifter till underbiträdet och hur underbiträdet uppfyller Dataförordningens krav
- Vidta lämpliga tekniska och organisatoriska åtgärder så att den personuppgiftsansvarige kan svara på enskilds begäran om att få utöva sina rättigheter
- Bistå den personuppgiftsansvarige med att se till att skyldigheterna fullgörs ifråga om säkerhetsåtgärder, konsekvensbedömningar, anmälan av personuppgiftsincidenter och information om sådana incidenter till de registrerade
- Radera eller återlämna alla personuppgifter till den personuppgiftsansvarige (beroende på vad den personuppgiftsansvarige väljer) när uppdraget avslutas och även radera alla kopior
- Ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att man fullgör alla skyldigheter som man har som biträde samt att möjliggöra och bidra till inspektioner och andra granskningar som den personuppgiftsansvarige vill genomföra
- Självmant anmäla personuppgiftsincidenter till tillsynsmyndigheten, samt meddela personuppgiftsansvarig om dessa.

9. Uppföljning och kontroll

För att säkerställa att samtliga ovanstående avsnitt – samt Dataskyddsförordningen i sin helhet – uppfylls, ska Forshaga kommuns arbete med Dataskyddsförordningen följas upp och kontrolleras med jämna mellanrum.

---

[37] Artikel 28 punkt 2
[38] Artikel 28 punkt 3
[39] Artikel 28 punkt 2
[40] Artikel 28 punkt 1 och punkt 5-10
[41] Artikel 28 punkt 4

9.1 Uppföljning av det interna arbetet

Det är nämnderna (personuppgiftsansvariga) som har ytterst ansvar för att följa upp det interna arbetet och säkerställa att arbetet följer denna riktlinje samt Dataskyddsförordningen i sin helhet. I nämndernas Riktlinjer/ hänvisning för hantering av Dataskyddsförordningen ska det beskrivas vilka rutiner verksamheterna har för att följa upp och säkerställa detta arbete. Specifik uppföljning av ett område inom Dataskyddsförordningen kan göras genom intern kontroll. Denna form av intern kontroll bör göras minst vartannat år, eller vid behov. Varje nämnd beslutar om vilket specifikt område den interna kontrollen ska följa upp. Den interna kontrollen ska alltid dokumenteras. Även informationsägare inom respektive nämnd ska arbeta aktivt för att deras nämnd upprätthåller säkerhetskraven som Dataskyddsförordningen föreskriver. Detta görs främst genom att informationsägare agerar rådgivande, och uppmärksammar då någon av de anställdas hantering av Dataskyddsförordningen verkar felaktig. På kommunövergripande nivå bör dataskyddsombud regelbundet följa upp kommunens efterlevnad av Dataskyddsförordningen, men minst vart femte år.

9.2 Regelbundna utbildningar

Forshaga kommun förutsätter att alla anställda inom kommunen tar ett eget ansvar för att leva upp till kommunens styrdokument samt Dataskyddsförordningen. För att efterleva denna vision ska därför alla nyanställda i Forshaga kommun genomgå en kort utbildning samt ett test vid anställning, som säkerställer att den anställda förstått kommunens ansvar enligt Dataskyddsförordningen. Efter godkänt test registreras kompetensen i personalsystemet. Samtliga kommunanställda ska därefter vid behov uppdatera sina kunskaper genom en liknande utbildning (test). Informationsägare kan vid behov initiera utbildningar och/eller tester. Detta gäller då de ser ett specifikt behov hos någon/några av de anställda. Slutligen ska kommunens dataskyddsombud, samt nämndernas informationsägare, fortbildas löpande eller vid behov.

9.3 Säkerställande av IT-system

Som angivet i avsnitt 3.2 ska alla IT-system som Forshaga kommun utformar/köper in utgå ifrån principerna om inbyggt dataskydd och dataskydd som standard (privacy by design och privacy by default)[42]. Dessa principer ska även genomsyra det dagliga och fortskridande arbetet/driften. IT system ska i första hand hållas efter av respektive systemägare – dessa ska säkerställa att IT systemet även efter utveckling/inköp följer principerna om inbyggt dataskydd och dataskydd som standard. Det är dock upp till alla anställda som använder IT-system att uppmärksamma om något inom IT systemet verkar bryta mot Dataskyddsförordningen och principerna om inbyggt dataskydd och dataskydd som standard. Det är också upp till alla anställda att se efter sitt eget användande, så att de inte bryter mot Dataskyddsförordningen. Detta gäller även om IT-systemet skulle visa sig innehålla så kallade ”säkerhetshål” sett till förordningen. Med andra ord ska alla anställda alltid eftersträva att behandla information (och då främst personuppgifter) på ett korrekt sätt[43] .

9.4 Gallring av information/personuppgifter

Samtliga anställda inom Forshaga kommun ansvarar för att regelbundet och konsekvent radera den information som inte längre uppfyller sitt angivna syfte. Detta gäller särskilt personuppgifter[44] , som alltid ska raderas om:

- Uppgifterna inte längre behövs för de ändamål som de samlades in för
- Behandlingen grundar sig på den enskildes samtycke, och denne återkallar samtycket

---

[42] Artikel 25
[43] Artikel 38 punkt 2
[44] Artikel 17

- Den enskilde motsätter sig personuppgiftsbehandling som sker inom ramen för kommunens verksamhetsutövning och *det inte finns berättigade skäl som väger tyngre än den enskildes intresse*
- Personuppgifterna har behandlats olagligt
- Radering krävs för att uppfylla en rättslig skyldighet
- Personuppgifterna avser barn och har samlats in i samband med att barnet skapar en profil i ett (socialt) nätverk Kommunens verksamheter ska ha rutiner för att säkerställa att icke-ändamålsenlig information gallras regelbundet. Gallring kan ske genom radering, arkivering enligt arkivlagen, eller Pseudonymisering. Verksamheternas rutiner för gallring ska beskrivas i Riktlinjer för hantering av Allmänna Dataskyddsförordningen.

  Tänk på nämndens dokumenthanteringsplan, grunden för dokumenthanteringsplan är Arkiv laget

9.4.1 Särskilt om arkiv

Enligt Arkivlagen[45] ska kommunens allmänna handlingar arkiveras. Denna lagstadgade behandling av personuppgifter *(kallad arkivändamål av allmänt intresse[46])* faller enligt Dataskyddsförordning under *behandling av känsliga personuppgifter krävs för särskilda arkivändamål*. Dataskyddsförordningen anger alltså att arkiverade personuppgifter inte behöver raderas[47].

Behandling av personuppgifter enligt arkivändamål av allmänt intresse ska dock föregås av att personuppgifterna (handlingarna) har behandlats enligt Dataskyddsförordningens principer för behandling. Vid behandling av personuppgifter enligt arkivändamål ska det också säkerställas att behandlingen omfattas av lämpliga skyddsåtgärder som omfattar både tekniska och organisatoriska åtgärder[48].

9.4.2 Särskilt om ostrukturerad behandling

Ostrukturerad behandling av personuppgifter ska som regel undvikas, då den omfattas av samma krav som övrig behandling av personuppgifter[49]. Om ostrukturerad behandling ändå sker, ska den ha laglig grund samt följa samma rutiner för gallring som övriga personuppgifter. Anställda får dock behandla och spara ostrukturerad behandling om behandlingen sker i löpande text som utgör utkast/minnesanteckning. Denna löptext får dock absolut inte lämnas ut (särskilt inte till tredje part), eller behandlas i mer än ett år. Dokument som behandlar ostrukturerad löptext ska dessutom på något sätt märkas upp, så att det syns att dokumentet behandlar personuppgifter. Detta kan exempelvis göras genom att tagga dokumentet. Notera att detta undantag inte gäller fritextfält i system som är byggda för att behandla personuppgifter (exempelvis register- eller journalsystem), då dessa alltid ska lämnas ut på begäran från registrerad.

9.5 Revidering av styrdokument

Forshaga kommuns Riktlinjeför hantering: Denna riktlinje ska följas upp vid behov, men minst en gång vartannat år, ansvarig för uppföljning är kommunledningsgruppen. Nämndernas Riktlinjer/hänvisning för hantering av personuppgifter ska följas upp vid behöv, men minst en gång om året. Ansvarig för uppföljning är nämndens informationsägare.

---

[45] Arkivlaget 1990:782
[46] *Artikel 5*
[47] Artikel 89
[48] Artikel 89 punkt 1
[49] Artikel 30