Kommunal författningssamling

Strategi för hantering av allmänna dataskyddsförordningen

Dokumenttyp	Strategi
Dokumentnamn	Strategi för hantering av allmänna dataskyddsförordningen
Nämnd	Kommunstyrelsen
Förvaltning	Kommunkansliet
Antagen	Kommunstyrelsen 2018-04-25
Paragraf	Kf § 58/2018
Ansvar	Säkerhetschef

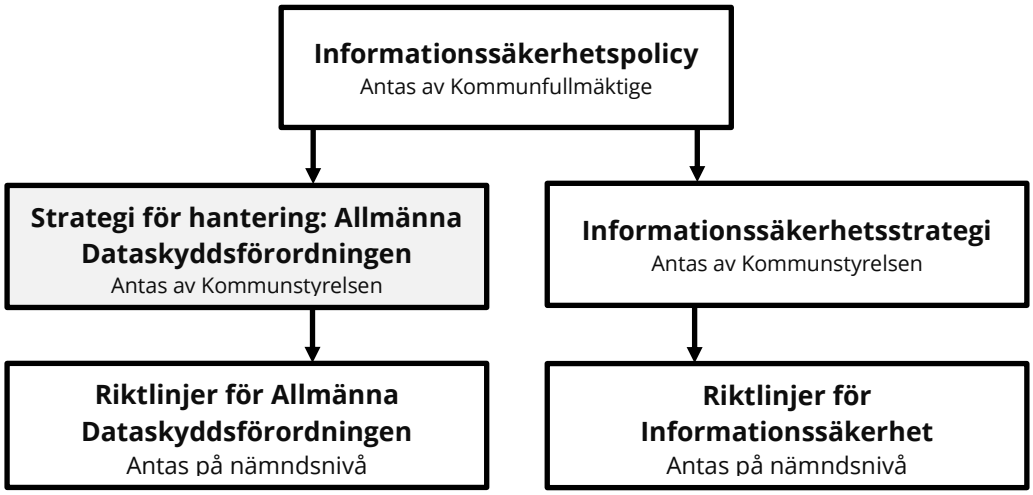
Strategi för hantering: Allmänna Dataskyddsförordningen

1. Inledning

Denna strategi utgör Kävlinge kommuns övergripande styrdokument för att hantera och implementera Allmänna Dataskyddsförordningen (EU:s förordning nr 2016/679), 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 strategi, vilket medför att det inte finns utrymme att besluta om lokala avvikande regler.

Kävlinge kommuns arbete med Informationssäkerhet i allmänhet och Allmänna Dataskyddsförordningen i synnerhet kan beskrivas enligt följande modell:



2. Syfte och mål

Syftet med denna strategi är att ange hur Kävlinge kommun säkerställer att de krav och villkor som anges i Allmänna Dataskyddsförordningen (förordning nr 2016/679) uppfylls.

Målet med denna strategi är att alla verksamheter där kommunen har ett huvudmannaansvar ska förstå hur de ska implementera Allmänna Dataskyddsförordningen (förordning nr 2016/679) i sin specifika verksamhet.

2.1 Avgränsning

Avgränsning i denna strategi sker gentemot sådant som faller utanför Allmänna Dataskyddsförordningens (förordning nr 2016/679) lagrum.

3. Vad innebär Allmänna Dataskyddsförordningen för kommunen?

Från och med den 25 maj 2018 gäller Allmänna Dataskyddsförordningen (EU:s förordning nr 2016/679, nedan kallad *Dataskyddsförordningen*). Dataskyddsförordningen, som också kallas GDPR efter engelskans General Data Protection Regulation, ersätter bland annat Personuppgiftslagen (1998:204) och innebär i korthet att kommunen måste föra register över sin hantering av personuppgifter, samt att alla incidenter som berör personuppgifter måste anmälas till Datainspektionen (nedan kallad *tillsynsmyndigheten*). Förordningen innebär också att konsekvensbedömningar måste göras innan nya behandlingar av personuppgifter sker, samt att ”missbruksregeln” försvinner (den anställda får inte längre behandla personuppgifter slentrianmässigt i exempelvis löptext och enkla listor). Nytt är också de höga sanktionsavgifter som kan utdömas mot de organisationer som missköter Dataskyddsförordningen.

3.1 Allmänt säkerhetskrav för kommunen

I enlighet med Dataskyddsförordningen[1] ska Kävlinge 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). Detta innebär att kommunen och dess anställda redan från upphandling ska ta hänsyn till de integritetsskyddsregler som Dataskyddsförordningen fastställer (se avsnitt 5), samt att anställda aktivt ser till att inte behandla personuppgifter eller annan känslig information i onödan. 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

Kävlinge kommuns definitioner följer Dataskyddsförordningens artikel 4.

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, vilka tidigare har omfattats av den så kallade ”missbruksregeln”. Likställs numera med övriga personuppgifter, och är således inte tillåtna utan laglig grund (se avsnitt 9.4.2).

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 onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

[1] Artikel 25

Personuppgiftsansvarig: 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. Också ansvarig för behandlingen av personuppgifter.

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 avkryptera räknas alltså *inte* som pseudonymiserade.

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 Dataskyddsförordningen 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

Kommunernas nämnder och bolag är enligt Dataskyddsförordningen fristående personuppgiftsansvariga[2]. Det innebär att Kommunstyrelsen, Bildningsnämnden, Miljö- och Byggnadsnämnden, Socialnämnden och Tekniska nämnden var för sig utgör personuppgiftsansvariga inom kommunens organisation. Personuppgiftsansvarig 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[3], samt att vid tillsyn kunna redovisa hur de säkerställer Dataskyddsförordningens krav och villkor[4].

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.

[2] Artikel 4 punkt 7
[3] Artikel 33
[4] Artikel 56

4.1 Nämndspecifika Riktlinjer för hantering

Varje nämnd ska upprätta minst en nämndspecifik *Riktlinjer för hantering av Allmänna Dataskyddsförordningen*, där den praktiska implementeringen av Dataskyddsförordningen beskrivs. På så sätt visar Kävlinge kommun hur Dataskyddsförordningens krav och villkor uppfylls och säkerställs utifrån varje nämnds specifika förutsättningar.

4.2 Nämndspecifika informationssäkerhetssamordnare

Samtliga nämnder ska utse minst en informationssäkerhetssamordnare som säkerställer att Dataskyddsförordningen, liksom kommunens styrdokument, efterlevs[5].

Nämndens informationssäkerhetssamordnare har som främsta uppgift att agera rådgivande och stöttande gentemot nämndens 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 nämnden får den utbildning de behöver för att leva upp till Dataskyddsförordningens krav

c) Säkerställa att nämndens behandling av personuppgifter registreras i kommunens registerföringssystem, samt att nämndens registerförda behandling av personuppgifter lever upp till lagstiftningen

d) Säkerställa att nämndens Riktlinjer för hantering av Allmänna Dataskyddsförordningen hålls aktuell och relevant

e) Kunna svara på frågor från anställda inom nämnden, kommunens dataskyddsombud, samt tillsynsmyndigheten, gällande nämndens arbete med Dataskyddsförordningen

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 artikel 37 är kommunens nämnder skyldiga att utse ett dataskyddsombud. I Kävlinge kommun är dataskyddsombudet tillika Säkerhetschefen.

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[6]. Dataskyddsombudet utgör också en rådgivande och stöttande instans gentemot nämndernas informationssäkerhetssamordnare.

5. Personuppgifter

Kävlinge kommuns behandling av personuppgifter ska alltid ske i enlighet med de principer som tas upp i Dataskyddsförordningen[7]. Vidare får Kävlinge kommuns faktiska behandling av personuppgifter enbart ske då minst ett av de lagstadgade skälen uppfylls[8].

Personer vars personuppgifter blir behandlade av Kävlinge 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 lagringen av

[5] Artikel 24 punkt 1 samt artikel 38 punkt 2
[6] Artikel 39
[7] Artikel 5 punkt 1
[8] Artikel 6

personuppgifter[9]. Informationen ska alltid förmedlas så att den registrerade förstår[10]. Den registrerade ska också få information om vilka rättigheter den enskilde har gentemot kommunen (se avsnitt 5.5.2). I tillämpliga fall ska den registrerade även meddelas om vilken tidsperiod personuppgifterna kommer lagras. Information om Kävlinge kommuns behandling av personuppgifter ska också finnas på kommunens hemsida.

För praktisk tillämpning av ovan skall-krav, hänvisas till respektive nämnds *Riktlinjer för hantering av Allmänna Dataskyddsförordningen*.

5.1 Allmänna principer för behandling av personuppgifter

Kävlinge kommun följer de principer som Dataskyddsförordningen anger för behandling av personuppgifter[11]. Principerna utgör ett grundkrav för kommunens behandling av personuppgifter, och ska alltid följas. Det är personuppgiftsansvariga som har ansvar för att principerna följs[12].

• **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.

• **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

Kävlinge kommun kräver att minst ett av nedanstående skäl[13] 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*

[9] Artikel 13 och 14
[10] Artikel 12 punkt 1
[11] Artikel 5
[12] Artikel 5 punkt 2
[13] Artikel 6

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 kan **enbart** användas för att motivera behandlingar inom kommunen, exempelvis mellan HR-avdelning och anställd. Behandlingen ska dock underbyggas med tydliga rutiner för användning.*

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”. Utgångspunkten är att all behandling av känsliga personuppgifter är förbjuden[14].

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 läggning[15]. 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[16]:

*[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]

[14] Artikel 9 punkt 1
[15] Artikel 9 punkt 1
[16] Artikel 9 punkt 2

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 *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, forsningsändamål 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.

5.3 Utlämnande av personuppgifter

Anställda inom Kävlinge kommun ska alltid säkerställa att *om ifall* personuppgifter måste lämnas ut, ska detta göras med hänsyn till personuppgifternas art och känslighet. Anställda ska hellre vara för restriktiva med utlämnade, än för generösa. Det enda undantaget 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 (2009:400)[17], 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[18], om inte uttryckligt samtycke getts[19]. Skulle den anställda ha svårt att avgöra huruvida den begärande parten har rätt till vissa personuppgifter, ska den anställda avböja att lämna ut så länge den begärande parten inte kan identifiera sig mer precist[20].

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[21]. Vid tillsyner eller liknande visning av personuppgifter måste en anställd från Kävlinge 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[22]. Denna information ska lämnas ut skyndsamt, men senast efter 30

[17] OSL kap 7
[18] Artikel 86
[19] Artikel 20 punkt 1
[20] Artikel 11 punkt 2
[21] Artikel 13-14 och Artikel 20
[22] Artikel 15

dagar[23]. 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[24]. 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 (se avsnitt 5.5.2)

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[25]. 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 Kävlinge 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

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 Kävlinge kommun ska klargöra *hur många* uppgifter som samlas in, vilken *rättslig grund* det finns för insamlandet (se avsnitt 5.2), 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.

[23] Artikel 12 punkt 3 och 4
[24] Artikel 15 punkt 3
[25] Artikel 35

5.5 Säkerhet vid behandling av personuppgifter

Utöver kommunens allmänna säkerhetskrav att följa principen om inbyggt dataskydd och dataskydd som standard (se avsnitt 3.1), ska kommunens anställda beakta särskild försiktighet när det kommer till behandlingen av personuppgifter[26]. 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 behandlingssystemen 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 konsevent 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 Särskilda säkerhetskrav vid användning av mobila enheter

Personuppgifter får inte behandlas på mobila enheter utanför den anställdas arbetsplats (gäller även av arbetsplatsen inköpta mobila enheter), såvida inte den externa platsen uppfyller Dataskyddsförordningens principer för hantering (avsnitt 5.1). Detta gäller även eventuellt wifi-nätverk den anställda kopplar upp sig mot.

Personuppgifter får inte heller behandlas på privatägda enheter, såvida inte denna/dessa uppfyller Dataskyddsförordningens principer för hantering (avsnitt 5.1) samt allmänna säkerhetskrav (avsnitt 3.1).

Den anställda får heller inte ladda ner icke-autentiserade applikationer och/eller applikationer med tveksamt innehåll till enheter som behandlar personuppgifter.

Vid användning av molntjänster ska dessa vara specifikt godkända för att hantera personuppgifter på ett säkert sätt, samt kunna uppfylla det allmänna säkerhetskravet (avsnitt 3.1).

5.5.2 Den enskildes rättigheter

Kävlinge kommun ska säkerställa att den enskildes rättigheter såsom fastställs i Dataskyddsförordningens artikel 15-22 uppfylls. Detta är en viktig säkerhetsåtgärd, och den praktiska implementeringen av rättigheterna förtydligas i respektive nämnds *Riktlinjer för hantering av Allmänna Dataskyddsförordningen*.

Rättigheterna är som följer:

[26] Artikel 32

• **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.

[Rätt till radering: Gäller ej vid rättslig förpliktelse, myndighetsutövning eller allmänt intresse. Notera dock avsnitt 9.4]

• **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 till, och den som har tagit emot personuppgifterna är då skyldig att underlätta en sådan överflyttning av personuppgifter.

• **Rätt att göra invändningar**: *Gäller enbart vid skäl 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[27]. 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[28].

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[29]. 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

[27] Artikel 77 och 78
[28] Artikel 82
[29] Artikel 33

nämnder[30]. Hur incidenter upptäcks, dokumenteras och anmäls till tillsynsmyndigheten definieras i nämndernas *Riktlinjer för hantering av Allmänna 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. Kävlinge kommun rekommenderar dock sina anställda att anmäla, snarare än att inte anmäla.

Samtliga incidentanmälningar ska innehålla (lättförståelig) information om:

• 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 personuppgiftansvariges 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[31]. 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[32]. Kävlinge 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.

Kävlinge 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

g) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som används för att skydda uppgifterna

[30] Artikel 33 punkt 1 och 2
[31] Artikel 34
[32] Artikel 30

7. Kommungemensamma behandlingar av personuppgifter

Kävlinge kommun delar tre verksamheter med Burlövs kommun och Staffanstorps kommun. Dessa tre verksamheter utgörs av löneservice (vilken Burlövs kommun har huvudsakligt ansvar för), IT-service (vilken Kävlinge kommun har huvudsakligt ansvar för) och geografisk information (geoinfo, vilken Staffanstorps kommun har huvudsakligt ansvar för).

För att säkerställa att personuppgifter hanteras på ett korrekt sätt av de tre 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 samtliga kommungemensamma verksamheter följer detta styrdokument samt Dataskyddsförordningen i sin helhet.

8. Personuppgiftsbiträden

Vid anlitande av personuppgiftsbiträde ska alltid ett skriftligt personuppgiftsbiträdesavtal tecknas[33]. Avtalet ska klargöra att personuppgiftsbiträdet och dess personal enbart får behandla personuppgifter enligt instruktion från den personuppgiftsansvarige[34], samt att biträdet inte får anlita andra biträden utan att ha fått ett skriftligt tillstånd av den personuppgiftsansvarige[35]. De biträden som kommunen anlitar ska dessutom kunna ge tillräckliga garantier för att deras behandling uppfyller kraven i Dataskyddsförordningen[36]. 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[37].

I avtal som Kävlinge 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 (se avsnitt 5.5)

• 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

[33] Artikel 28 punkt 2
[34] Artikel 28 punkt 3
[35] Artikel 28 punkt 2
[36] Artikel 28 punkt 1 och punkt 5-10
[37] Artikel 28 punkt 4

• 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 Kävlinge kommuns arbete med Dataskyddsförordningen följas upp och kontrolleras med jämna mellanrum.

9.1 Uppföljning av det interna arbetet

Det är ytterst nämnderna (personuppgiftsansvariga) som har ansvar för att följa upp det interna arbetet och säkerställa att arbetet följer denna strategi samt Dataskyddsförordningen i sin helhet. I nämndernas *Riktlinjer för hantering av Allmänna 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 informationssäkerhetssamordnarna inom respektive nämnd ska arbeta aktivt för att deras nämnd upprätthåller säkerhetskraven som Dataskyddsförordningen föreskriver. Detta görs främst genom att informationssäkerhetssamordnarna agerar rådgivande, och uppmärksammar då någon av de anställdas hantering av Dataskyddsförordningen verkar felaktig.

På kommunövergripande nivå bör kommunrevisionen regelbundet följa upp kommunens efterlevnad av Dataskyddsförordningen, men minst vart femte år.

9.2 Regelbundna utbildningar

Kävlinge 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 Kävlinge kommun genomgå en kort utbildning samt ett test vid anställning, som säkerställer att den anställda förstått kommunens ansvar enligt Dataskyddsförordningen.

Det godkända testet ska sparas i den anställdas personalakt.

Samtliga kommunanställda ska därefter regelbundet uppdatera sina kunskaper genom ett liknande test. Denna fortbildning ska ske minst en gång vartannat år genom en e-learningportal.

Informationssäkerhetssamordnarna 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 kommunens informationssäkerhetssamordnare, fortbildas minst en gång varje år eller vid behov.

9.3 Säkerställande av IT-system

Som angivet i avsnitt 3.2 ska alla IT-system som Kävlinge kommun utformar/köper in utgå ifrån principerna om inbyggt dataskydd och dataskydd som standard (privacy by design och privacy by

default)[38]. 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[39].

9.4 Gallring av information/personuppgifter

Samtliga anställda inom Kävlinge kommun ansvarar för att regelbundet och konsekvent radera den information som inte längre uppfyller sitt angivna syfte. Detta gäller särskilt personuppgifter[40], 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

• 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*.

9.4.1 Särskilt om arkiv

Enligt Arkivlagen (1990:782) ska kommunens allmänna handlingar arkiveras. Denna lagstadgade behandling av personuppgifter (kallad *arkivändamål av allmänt intresse*[41]) faller enligt Dataskyddsförordning under *behandling av känsliga personuppgifter/j) krävs för särskilda arkivändamål*. Dataskyddsförordningen anger alltså att arkiverade personuppgifter inte behöver raderas[42].

Behandling av personuppgifter enligt arkivändamål av allmänt intresse ska dock föregås av att personuppgifterna (handlingarna) har behandlats enligt Dataskyddsförordningens principer för behandling (avsnitt 5.1). Vid behandling av personuppgifter enligt arkivändamål ska det också säkerställas att behandlingen omfattas av lämpliga skyddsåtgärder som omfattar både tekniska och organisatoriska åtgärder[43].

[38] Artikel 25
[39] Artikel 38 punkt 2
[40] Artikel 17
[41] Artikel 5
[42] Artikel 89
[43] Artikel 89 punkt 1

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[44]. 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

Kävlinge kommuns *Strategi för hantering: Allmänna Dataskyddsförordningen* ska följas upp vid behov, men minst en gång vartannat år. Ansvarig för uppföljning är säkerhetsenheten.

Nämndernas *Riktlinjer för hantering av Allmänna Dataskyddsförordningen* ska följas upp vid behov, men minst en gång om året. Ansvarig för uppföljning är nämndens informationssäkerhetssamordnare.

[44] Artikel 30