



Riktlinjer för dataskydd och hantering av personuppgifter

Flik 8.43





Dokumenttyp	Riktlinje
Dokumentnamn	Riktlinjer för dataskydd och hantering av personuppgifter
Fastställd första gången	2026-06-15 § 46
Senast reviderad	
Giltighetstid	Tills vidare
Beslutande	Kommunfullmäktige
Processägare	Kanslichef
Detta dokument gäller för	Vingåkers kommun

Innehåll

1.	Inledning och syfte	4
2.	Dokumentet gäller för	4
3.	Ansvarsfördelning och roller.....	4
3.1	Personuppgiftsansvar	4
3.2	Särskilt om kommunstyrelsen.....	5
3.3	När flera nämnder behandlar samma personuppgifter	5
3.4	Personuppgiftsbiträde	5
3.5	Dataskyddsombud.....	5
3.6	Dataskyddssamordnare	6
4.	Registerförteckning	6
5.	Konsekvensbedömning	7
6.	Personuppgiftsincident	7
7.	Personuppgiftsbiträdesavtal.....	7
8.	Sekretess.....	7
9.	Gallring och bevarande av personuppgifter	8
10.	De registrerades rättigheter	8
11.	Inspektion och granskning	9

1. Inledning och syfte

De här riktlinjerna tydliggör hur Dataskyddsförordningens krav förverkligas i Vingåkers kommun. Syftet är att säkerställa att kommunen hanterar personuppgifter korrekt och likvärdigt, och att visa för allmänhet och anställda att deras personuppgifter hanteras på ett respektfullt sätt.

Samtidigt som kommunens nämnder är självständiga personuppgiftsansvariga är de också en del av Vingåkers kommun. För att kunna utföra kommunens uppdrag är det nödvändigt att lösa vissa uppgifter gemensamt och ha vissa gemensamma digitala system.

Riktlinjerna tydliggör nämndernas ansvar för olika uppgifter enligt Dataskyddsförordningen samt deras skyldigheter gentemot varandra och de registrerade.

2. Dokumentet gäller för

Vingåkers kommuns nämnder, styrelser, bolag, förvaltningar, verksamheter och medarbetare. Likaså av andra personer som arbetar på uppdrag av eller under översyn av Vingåkers kommun.

3. Ansvarsfördelning och roller

Dataskyddsförordningen kräver ett tydligt fastställande om vem som bär ansvar. I Vingåkers kommun är varje nämnd och styrelse personuppgiftsansvariga för sina personuppgiftsbehandlingar.

3.1 Personuppgiftsansvar

Varje nämnd och styrelse inom Vingåkers kommun är personuppgiftsansvarig för behandlingar av personuppgifter inom sitt verksamhetsområde.

Nämnderna ansvarar för att kraven som ställs på personuppgiftsansvariga i Dataskyddsförordningen uppfylls. Ansvaret innebär en yttersta skyldighet att tillse att gällande lagstiftning efterlevs genom att bland annat:

- Fastställa ändamål och syfte med behandling av personuppgifter, innan behandlingen börjar.
- Säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med nödvändig säkerhet.
- Kunna visa att krav i lagstiftning är uppfyllda genom noggrann dokumentation.
- Säkerställa att riskanalyser genomförs och dokumenteras.
- Säkerställa att det görs konsekvensbedömningar om behandlingar sannolikt medför en hög risk för den registrerades integritet.
- Säkerställa att personuppgiftsincidenter rapporteras till Integrationsmyndigheten (IMY).

- Tillgodose registrerades rättigheter gällande information, tillgång (registerutdrag), rättning, begränsning, dataportabilitet och invändning.
- Föra register över behandlingar av personuppgifter i för ändamålet avsett register (VingSys).

3.2 Särskilt om kommunstyrelsen

Kommunstyrelsen har ett ansvar för att leda, samordna och ha uppsikt över kommunens arbete med att uppfylla kraven i Dataskyddsförordningen. Kommunstyrelsen har genom sin uppsiktsplikt över nämnderna ett särskilt ansvar för kommunens behandling av personuppgifter.

Kommunens myndigheter är självständiga personuppgiftsansvariga, samtidigt som de tillhör samma organisation och är underordnade kommunfullmäktiges beslutanderätt. För att utföra kommunens uppdrag effektivt och likvärdigt är det nödvändigt att vissa saker görs gemensamt för alla nämnders verksamheter, till exempel gällande ekonomi och löner. I Vingåkers kommun är kommunstyrelsen personuppgiftsansvarig när behandlingen av personuppgifter görs gemensamt.

3.3 När flera nämnder behandlar samma personuppgifter

När två eller flera personuppgiftsansvariga gemensamt beslutar om ändamål och medel för behandlingen kallas det för gemensamt personuppgiftsansvar. Varje nämnd ansvarar för den del av behandlingen som ligger inom den egna verksamheten enligt reglementet och får utföra de behandlingsåtgärder som behövs för att genomföra sina respektive uppdrag.

3.4 Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i Dataskyddsförordningen och ska säkerställa att den registrerades rättigheter skyddas. Ett personuppgiftsbiträde och dess medarbetare får bara behandla personuppgifter enligt instruktion från den personuppgiftsansvarige.

3.5 Dataskyddsombud

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen.

Det innebär bland annat att

- samla in information om hur personuppgiftsansvarig behandlar personuppgifter
- kontrollera att personuppgiftsansvarig följer bestämmelser och interna styrdokument
- informera och ge råd inom organisationen

Dataskyddsombudet ska också

- ge råd om konsekvensbedömningar
- vara kontaktperson gentemot Integritetsskyddsmyndigheten (IMY)

- samarbeta med Integritetsskyddsmyndigheten (IMY), till exempel vid inspektioner.

Vingåkers kommuns dataskyddsombud är Sydarkivera.

3.6 Dataskyddssamordnare

Dataskyddssamordnaren är en stödfunktion för personuppgiftsansvarig nämnd, förvaltningens ledning och verksamhet. Ansvar för att lagstiftning efterlevs vilar alltid på personuppgiftsansvarig och ansvaret kan inte delegeras.

Dataskyddssamordnaren har bland annat följande uppgifter:

- Behandlingsregistret.
- Samordna och besvara registrerades begäran om att utöva sina rättigheter som exempelvis begäran om registerutdrag, radering och invändning.
- Följa upp att nödvändiga rutiner och instruktioner finns tillgängliga och är kända inom den egna verksamheten.
- Vara stöd vid upprättande av personuppgiftsbiträdesavtal, konsekvensbedömning avseende dataskydd och utredning av personuppgiftsincidenter.
- Vara stöd vid bedömning av om en personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten (IMY) och om de registrerade ska informeras om incidenten.
- Vara förvaltningens eller bolagets representant i det kommunövergripande nätverket för dataskydd.
- Samordna förvaltningens arbete med uppföljning och egenkontroll av dataskyddet.
- Samarbeta med dataskyddsombudet och fungera som länk mellan dataskyddsombudet och personuppgiftsansvarig.
- Omvärldsbevaka kring personuppgiftsfrågor generellt och utifrån det egna verksamhetsområdet.
- Rådfråga och samråda med dataskyddsombudet för verksamhetens räkning, bland annat i samband med konsekvensbedömning avseende dataskydd.

4. Registerförteckning

Personuppgiftsansvariga är skyldiga att föra ett register över sina behandlingar av personuppgifter.

Behandlingsregistret ska upprättas skriftligen, vara tillgängligt i elektroniskt format och hållas uppdaterat. På begäran ska registret göras tillgängligt för Integritetsskyddsmyndigheten (IMY). Vad som ska finnas med i registret beskrivs i artikel 30 i Dataskyddsförordningen.

Registrering ska ske i kommunens system (VingSys).

5. Konsekvensbedömning

Om en behandling sannolikt leder till en hög risk för fysiska personers fri- och rättigheter ska en konsekvensbedömning avseende dataskydd göras. Konsekvensbedömningen ska göras innan behandlingen påbörjas och dataskyddsombudet ska rådfrågas. Konsekvensbedömningen görs för att:

- ta reda på vilka risker som finns med att behandla personuppgifter
- ta fram rutiner och åtgärder för att sänka dessa risker
- visa att man uppfyller Dataskyddsförordningens krav.

För att avgöra om en behandling sannolikt leder till en hög risk ska en tröskelanalys göras. Tröskelanalysen ska dokumenteras. Analysen utgår från fastställda kriterier. Om fler än två av kriterierna är uppfyllda ska en konsekvensbedömning som huvudregel genomföras.

6. Personuppgiftsincident

I Dataskyddsförordningen definieras en personuppgiftsincident som ”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”.

Alla organisationer är enligt Dataskyddsförordningen skyldiga att ha rutiner för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter.

Varje förvaltning ska kunna upptäcka och rapportera personuppgiftsincidenter som sker inom den egna verksamheten.

7. Personuppgiftsbiträdesavtal

Varje nämnd ska teckna personuppgiftsbiträdesavtal (PUB-avtal) när denna uppdrar åt ett externt personuppgiftsbiträde att behandla uppgifter för nämndens räkning.

Vem som kan teckna personuppgiftsbiträdes avtal ska framgå av respektive förvaltnings delegationsordning.

Personuppgiftsbiträdes behandling av personuppgifter ska regleras av personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige.

Det åligger varje personuppgiftsansvarig att säkerställa att personuppgiftsbiträdesavtal (PUB-avtal) tecknas med aktörer utanför kommunens organisation som ska behandla personuppgifter för kommunens räkning. Personuppgiftsansvarig ska även hålla PUB-avtalen samlade och ordnade i enlighet med aktuell informationshanteringsplan.

8. Sekretess

Inom kommunen gäller tystnadsplikt enligt offentlighets- och sekretesslagens (OSL) bestämmelser. Utöver det ska personuppgifter alltid behandlas varsamt och konfidentiellt. Behörighet till

personuppgifter ska bara ges till anställda som behöver tillgång till uppgifterna för att utföra sina arbetsuppgifter. Det ska finnas rutiner för att regelbundet granska vilka som har tillgång till personuppgifter och ta bort behörigheter som inte längre behövs.

När ett externt personuppgiftsbiträde eller underbiträde anlitas ska det säkerställas att de personer som har tillgång till personuppgifter omfattas av lagstadgad eller avtalsrättslig tystnadsplikt. Avtalsrättslig tystnadsplikt är inte alltid tillräcklig. En bedömning måste göras utifrån den aktuella informationen.

9. Gallring och bevarande av personuppgifter

Vid gallring och arkivering av personuppgifter ska gällande lagstiftning och kommunens informationshanteringsplan gällande arkivering och informationsförvaltning tillämpas.

När ett externt personuppgiftsbiträde eller underbiträde anlitas ska det säkerställas att biträdet är skyldig att radera eller återlämna alla personuppgifter och radera eventuella kopior när personuppgiftsbehandlingen upphör.

10. De registrerades rättigheter

De personer vars personuppgifter behandlas kallas för de registrerade. Enligt Dataskyddsförordningen har de registrerade ett antal rättigheter gällande sina personuppgifter. Vingåkers kommun har en gemensam e-tjänst för att använda rätten till:

- tillgång (registerutdrag),
- rättelse,
- återkallelse av samtycke,
- begränsning,
- dataportabilitet,
- invändning mot behandling, samt
- radering.

Registrerade som inte kan använda sig av e-tjänsten har möjlighet att få hjälp inom ramen för kommunens serviceskyldighet.

Flera av de registrerades rättigheter gäller i begränsad omfattning i offentlig förvaltning. En begäran från den registrerade ska prövas och den registrerade ska få ett beslut som kan överklagas om begäran avslås. Vilka beslut som kan överklagas framgår av 7 kap. 2 § dataskyddslagen.

En begäran som riktar sig mot flera personuppgiftsansvariga i kommunen handläggs gemensamt av kanslienheten. Beslut måste dock fattas av varje personuppgiftsansvarig för sig.

11. Inspektion och granskning

Kommunens samlade personuppgiftsbehandling granskas genom ordinarie rutiner för intern kontroll och revision. Därutöver ska varje personuppgiftsansvarig nämnd och styrelse bedriva ett systematiskt egenkontrollarbete. Granskning görs även av kommunens dataskyddsombud. Samtliga nämnder ska kunna tillhandahålla den information som behövs för granskning av personuppgiftsbehandlingen.

Kommunstyrelsen och Kanslienheten har ett utökat ansvar för att kunna redovisa att de digitala tjänster och system som används kommunövergripande uppfyller de krav som ställs och att personuppgiftsbehandlingen följs upp löpande.

Alla personuppgiftsbiträdesavtal som ingås med externa parter ska vara utformade så att biträden och underbiträden är skyldiga att tillhandahålla den information som behövs för att granska så att de krav som ställs uppfylls.