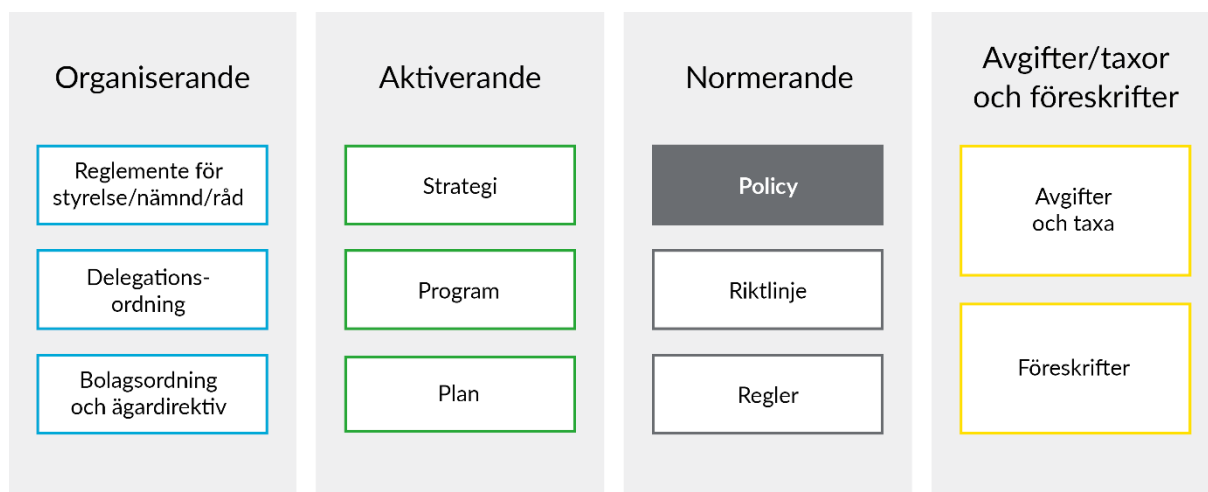




# Dataskyddspolicy för Vingåkers kommun

Flik 7.31





|                                  |                                       |
|----------------------------------|---------------------------------------|
| <b>Dokumenttyp</b>               | Policy                                |
| <b>Dokumentnamn</b>              | Dataskyddspolicy för Vingåkers kommun |
| <b>Fastställt första gången</b>  | 2026-06-15 § 45                       |
| <b>Senast reviderad</b>          |                                       |
| <b>Giltighetstid</b>             | tills vidare                          |
| <b>Beslutande</b>                | Kommunfullmäktige                     |
| <b>Processägare</b>              | Kanslichef                            |
| <b>Detta dokument gäller för</b> | Vingåkers kommun                      |

# Innehåll

|     |                                                          |   |
|-----|----------------------------------------------------------|---|
| 1.  | Syftet med denna policy .....                            | 4 |
| 2.  | Omfattning .....                                         | 4 |
| 3.  | Gällande dataskyddslagstiftning.....                     | 4 |
| 4.  | Viktiga begrepp och definitioner .....                   | 5 |
| 5.  | Ändamål med behandling av personuppgifter.....           | 6 |
| 6.  | Dataskyddsförordningens grundläggande principer.....     | 6 |
| 7.  | Roller.....                                              | 7 |
| 7.1 | Personuppgiftsansvarig.....                              | 7 |
| 7.2 | Dataskyddsombud.....                                     | 7 |
| 7.3 | Dataskyddsansvarig .....                                 | 7 |
| 7.4 | Dataskyddssamordnare .....                               | 7 |
| 7.5 | Medarbetare .....                                        | 7 |
| 8.  | Personuppgiftsbehandlingar mellan myndighetsgränser..... | 8 |
| 9.  | Kompletterande styrdokument .....                        | 8 |

## 1. Syftet med denna policy

Alla individer vars personuppgifter behandlas inom ramen för Vingåkers kommuns verksamhet ska vara trygga med hur deras personuppgifter hanteras.

Denna policy ska säkerställa att Vingåkers kommun:

följer gällande lagstiftning

- lagrar och hanterar personuppgifter på ett korrekt och enhetligt sätt
- kommunicerar tydligt och öppet gällande hur personuppgifter hanteras i verksamheten
- kan tillmötesgå anställdas, kommuninvånarens och andras intressenters rättigheter
- skyddar den egna verksamheten mot hot och därmed minimerar integritetsrisker

## 2. Omfattning

Policyn har tagits fram av Vingåkers kommuns dataskyddssamordnare och omfattar all behandling av personuppgifter som utförs inom organisationen.

Denna policy gäller samtliga verksamheter inom Vingåkers kommun. Policyn ska kompletteras med riktlinjer och rutiner inom dataskydd samt andra specifika verksamhetsområden.

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

## 3. Gällande dataskyddslagstiftning

Hantering av och skyddet för personuppgifter regleras övergripande av EU:s allmänna dataskyddsförordning (GDPR – Europaparlamentets och rådets förordning [EU] 2016/679) samt kompletterande svensk lagstiftning i form av den kompletterande dataskyddslagen och tillhörande förordning (SFS 2018:218 och SFS 2018:219).

Ytterligare relevant lagstiftning kan tillkomma i form av exempelvis registerförfattningar inom specifika branschområden.

Integritetsskyddsmyndigheten (IMY) är tillsynsmyndighet gällande personuppgiftsrelaterade ärenden.

## 4. Viktiga begrepp och definitioner

Denna policy rör hantering av personuppgifter. Personuppgifter är all information som kan användas för att identifiera en nu levande enskild person, direkt eller indirekt. Begreppet personuppgifter inkluderar, men är inte begränsat till:

- Namn
- Personnummer
- E-postadress
- Telefonnummer
- IP-adress
- Kundnummer
- Bilder (på personer)

I uttrycket behandling av personuppgifter inkluderas allt som görs där personuppgifter förekommer, exempelvis administration av, kommunikation med och lagring av sådana uppgifter för olika ändamål och i olika sammanhang.

I den mån känsliga personuppgifter förekommer i Vingåkers kommuns verksamhet gäller särskilda regler. Känsliga personuppgifter är:

- Uppgifter som avslöjar ras eller etniskt ursprung,
- Uppgifter som avslöjar politiska åsikter,
- Uppgifter som avslöjar religiös eller filosofisk övertygelse,
- Uppgifter om medlemskap i fackförening,
- Uppgifter om hälsa,
- Uppgifter om sexualliv eller sexuell läggning.
- Genetiska uppgifter och
- Biometriska uppgifter för att entydigt identifiera en fysisk person.

Observera att även uppgifter som indirekt avslöjar känslig information av detta slag inkluderas.

Nämnderna i Vingåkers kommun är personuppgiftsansvariga för de flesta av de personuppgiftsbehandlingar som förekommer i verksamheten.

Kommunstyrelsen anses vara personuppgiftsansvarig för kommunövergripande personuppgiftsbehandlingar. Med detta menas att kommunstyrelsen är den som är ytterst ansvarig för personuppgifterna, och som bestämmer över ändamål och medel.

Roller och ansvarsfördelning mellan organisationen och eventuella personuppgiftsbiträden ska framgå för varje behandling i registerförteckningen (VingSys).

## 5. Ändamål med behandling av personuppgifter

Vingåkers kommun behandlar en stor mängd personuppgifter för olika typer av ändamål. Vingåkers kommun behandlar i många fall personuppgifter i ett allmänt intresse och myndighetsutövning för att leva upp till lagar och förordningar. I andra fall kan personuppgiftsbehandlingar bygga på avtalsförhållanden, exempelvis gällande anställdas personuppgifter. Vingåkers kommun kan också behöva behandla personuppgifter genom rättsliga förpliktelser. Viss personuppgiftsbehandling kan ske genom att enskild har samtyckt till att Vingåkers kommun får behandla personuppgifter. Samtycke som rättslig grund för personuppgiftsbehandling ska ske restriktivt eftersom ett samtycke kan återkallas när som helst samt att registrerade ofta står i beroendeställning till myndigheter.

## 6. Dataskyddsförordningens grundläggande principer

Dataskyddsförordningen bygger på ett antal principer. Dessa principer beskriver de skyldigheter som organisationer måste följa när personuppgifter behandlas. Dataskyddsförordningens grundläggande principer är att personuppgiftsansvarig:

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter. Personuppgifter måste behandlas på ett lagligt, korrekt och öppet sätt (principen om laglighet),
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål och får inte behandlas för något ändamål som är oförenligt med dessa ändamål (principen om ändamålsbegränsning)
- inte behandlar fler personuppgifter än vad som är nödvändigt för ändamålet (principen om uppgiftsminimering)
- ska se till att personuppgifterna är korrekta (principen om riktighet),
- ska radera personuppgifterna när de inte längre behövs (principen om lagringsminimering),
- ska skydda personuppgifterna på ett sätt som säkerställer lämpligt skydd, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs (principen om integritet och konfidentialitet),
- ska kunna visa att man lever upp till dataskyddsförordningen och på vilket sätt det görs (principen om ansvarsskyldighet).

## **7. Roller**

### **7.1 Personuppgiftsansvarig**

Inom kommunen är det nämnd, styrelse eller bolagsstyrelse som är personuppgiftsansvarig, vilket innebär att de har ansvaret för att personuppgifter behandlas lagligt, säkert och i övrigt korrekt. Personuppgiftsansvarig kan överlåta det operativa arbetet kring personuppgifter genom att besluta om delegation, men personuppgiftsansvaret kan aldrig överlåtas.

### **7.2 Dataskyddsombud**

Vingåkers kommuns dataskyddsombud är Sydarkivera. Dataskyddsombudets arbetsuppgifter och ställning styrs av lagstiftning. Funktionen ska agera självständigt och får inte ta emot instruktioner eller bli föremål för sanktioner för att ha utfört sina arbetsuppgifter. Dataskyddsombudet rapporterar till högsta ledningen såsom nämnd eller styrelse.

### **7.3 Dataskyddsansvarig**

Vingåkers kommun ska utse en ansvarig för lokal samordning inom området dataskydd. Dataskyddsansvarig har regelbunden kontakt med dataskyddsombud och förmedlar information.

### **7.4 Dataskyddssamordnare**

Varje förvaltning utser en eller flera dataskyddssamordnare för att stödja förvaltningen i dataskyddsarbetet. Kommunens dataskyddssamordnare har ett lokalt nätverk för samverkan och samarbete kring dataskydd.

Det är viktigt att dataskyddssamordnaren har god kännedom om förvaltningen och dess olika processer och verksamheter. Varje dataskyddssamordnare behöver få nödvändig kompetens inom dataskyddsområdet genom internutbildning. Dataskyddssamordnaren ska ha förutsättningar för att kunna utföra uppdraget. Tid, kompetens och mandat bedöms utifrån vilka områden som ska prioriteras inom respektive förvaltning.

### **7.5 Medarbetare**

Medarbetarna har ett ansvar att följa Vingåkers kommuns styrdokument inom dataskydd. Man har som medarbetare också ansvar att vara uppmärksam på bister och fel gällande personuppgiftshantering. Medarbetare ska även genomföra de utbildningar inom dataskydd som Vingåkers kommun tillhandahåller.

## **8. Personuppgiftsbehandlingar mellan myndighetsgränser**

Dataskyddspolicyn reglerar även behandling av personuppgifter nämnder emellan. Det innebär att personuppgifter kan flöda över myndighetsgränser och hanteras av nämnd där annan nämnd är personuppgiftsansvarig. Detta kan ske under förutsättning att de grundläggande principerna i dataskyddsförordningen efterlevs och att samtliga behandlingar har rättslig grund.

## **9. Kompletterande styrdokument**

Vidare riktlinjer och instruktioner som rör Vingåkers kommuns personuppgiftsbehandling finns bland annat i följande dokument:

- Informationssäkerhetspolicy för Vingåkers kommun
- Policy för IT
- Riktlinjer för dataskydd och hantering av personuppgifter för Vingåkers kommun
- Cybersäkerhetspolicy och -riktlinjer