

Riktlinje

Gullspångs kommun

Riktlinje för hantering av personuppgifter



Beslutad av: Kommunfullmäktige

Datum och paragraf: 2025-10-30 § 98

Dokumentansvarig:
Informationssäkerhetsstrateg

Gäller från: 2025-11-01

Diarienummer: 2025-00166



**GULLSPÅNGS
KOMMUN**

Innehåll

Riktlinjer för hantering av personuppgifter.....	3
Inledning.....	3
Vanliga begrepp och definitioner.....	3
Ansvar och roller.....	5
Personuppgiftsansvarig.....	5
Informationssäkerhetsstrateg.....	6
Informationssäkerhetssamordnare.....	6
Informationssäkerhetsgrupp.....	7
Övriga chefer och medarbetare.....	7
Dataskyddsombud.....	7
Grundläggande principer vid behandling av personuppgifter.....	8
Den registrerades rättigheter.....	9
Rätt till information.....	10
Rätt till rättelse.....	10
Rätt till radering.....	10
Övriga rättigheter.....	10
Registerförteckning.....	11
Säkerhetsåtgärder vid personuppgiftsbehandling.....	11
Personuppgiftsincidenter.....	11
Personuppgifter i e-post.....	11
Publicering av personuppgifter på internet.....	12
Publicering av fota/film.....	12
Dataskydd i upphandling.....	13
Introduktion av nyanställda.....	13

Riktlinje för hantering av personuppgifter

Denna riktlinje gäller för kommunens samtliga verksamheter, förtroendevalda och anställda. Kommunala bolag ska så långt det är möjligt utifrån aktiebolagslagen följa dessa riktlinjer. För kommunala verksamheter finns det inte utrymme att besluta om lokala regler som avviker från dessa riktlinjer.

Inledning

EU:s dataskyddsförordning (2016/679) trädde i kraft den 25 maj 2018 och reglerar både offentliga och privata organisationers behandling av personuppgifter. Ett av syftena med dataskyddsförordningen är att skydda enskildas grundläggande fri- och rättigheter, särskilt deras rätt till skydd av personuppgifter.

Dataskyddsförordningen är underordnad i förhållande till vissa andra författningar, vilket innebär att om det i annan lag eller förordning finns bestämmelser som avviker från dataskyddsförordningen, ska dessa bestämmelser tillämpas i stället, till exempel behandling av personuppgifter enligt socialtjänsten. Dataskyddsförordningen gäller inte heller om det skulle strida mot tryck- eller yttrandefriheten. Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att förordningen följs, vilket i praktiken ofta innebär ökade krav på dokumentation och interna rutiner.

Kommunens hantering och behandling av personuppgifter handlar om att tillgodose individens rättssäkerhet och integritetsskydd i samband med personuppgiftsbehandling.

Syftet med denna riktlinje är att sätta de ramar som kommunens verksamheter och bolag behöver iaktta vid hantering av personuppgifter. Detta dokument ska sedan kompletteras med rutiner som på ett mera detaljerat sätt stödjer verksamheterna löpande arbete med hanteringen av personuppgifter.

Vanliga begrepp och definitioner

Begrepp	Definition
Anonymisering	Med anonyma uppgifter menas personuppgifter som har gjorts anonyma på ett sådant sätt så att den registrerade inte längre kan identifieras (jämför med pseudonymisering längre ner). Behandling av personuppgifter som resulterar i anonym information kallar vi för anonymisering. Dataskyddsförordningen gäller inte för anonym information, men att anonymisera personuppgifter är en personuppgiftsbehandling som dataskyddsförordning ska tillämpas på.
Behandling av personuppgifter	Behandling av personuppgifter omfattar alla åtgärder som vidtas med personuppgifter, såsom insamling, registrering, organisering, lagring, bearbetning, ändring, framtagning, fotografering, läsning, användning, utlämning, spridning eller tillhandahållande på annat sätt. Även vid justering eller sammanföring, radering eller förstöring är det fråga om behandling av personuppgifter.

Biometriska uppgifter	Är en persons fysiska, fysiologiska eller beteendemässiga egenskaper som gör det möjligt att identifiera människor, exempelvis genom fingeravtryckskanning, ansiktsskanning eller ögonskanning.
Direkta personuppgifter	Direkta personuppgifter är exempelvis namn och personnummer, alltså sådan information som direkt pekar ut en individ utan att man behöver tillföra ytterligare information. Det är lätt att förstå att de är personuppgifter.
Integritetskänsliga personuppgifter	Det finns många andra typer av personuppgifter som är särskilt skyddsvärda. Det kan exempelvis vara personnummer, löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter (till exempel uppgifter från utvecklingssamtal eller resultat från personlighetstester), information som rör någons privata sfär eller uppgifter om sociala förhållanden.
Indirekta personuppgifter	De indirekta personuppgifterna är lite mer komplicerade. Det rör sig om uppgifter som pekar ut en individ om man kompletterar dem med annan information.
Känsliga personuppgifter	En särskild kategori av personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning, genetiska uppgifter eller biometriska uppgifter som används för att entydigt identifiera en person.
Personuppgift	All information som direkt eller indirekt kan kopplas till en enskild fysisk individ som är i livet, till exempel namn, adress och personnummer. Även information som beskriver någon eller på annat sätt kan härledas till en enskild individ såsom registreringsnummer på fordon, filmer, bilder, IP-nummer och cookies. Även information som har kodats, krypterats eller pseudonymiserats men som kan hänföras till en enskild individ med hjälp av kompletterande uppgifter klassas som personuppgifter och dataskyddsförordningen är tillämplig på dessa.
Personuppgiftsansvarig	Personuppgiftsansvarig (PuA) är den som bestämmer för vilka ändamål som uppgifterna ska behandlas och hur behandlingen ska gå till. Respektive nämnd och styrelse är personuppgiftsansvarig i kommunen.
Personuppgiftsbiträde	Ett personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning, där personuppgiftsansvarige bestämmer ändamålet med behandlingen. Ett personuppgiftsbiträde finns alltid utanför kommunen. Om kommunen ska anlita ett personuppgiftsbiträde ska det säkerställas att biträdet kan ge tillräckliga garantier om att upprätthålla lämplig teknisk och organisatorisk säkerhet i enlighet med dataskyddslagstiftningen. Personuppgiftsbitrådets behandling av personuppgifter ska regleras i ett personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige.

Personuppgiftsregister	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
Pseudonymisering	Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person. Vid behandling av pseudonymiserade personuppgifter är dataskyddsförordningen fortfarande tillämplig, även om risken för att identifiera en person är mindre.
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 personuppgiftsbitrådets direkta ansvar är behöriga att behandla personuppgifterna

Ansvar och roller

Personuppgiftsansvarig

Varje nämnd och kommunalt bolag är personuppgiftsansvarig för behandling av personuppgifter inom sitt verksamhetsområde. Nämnderna och bolagsstyrelserna har det yttersta ansvaret för att dataskyddsförordningen efterlevs. Ansvaret gäller såväl uppgifter om anställda och förtroendevalda som uppgifter om medborgare, barn/elever, brukare/klienter och kunder. Det gäller oavsett om personuppgifterna behandlas internt inom kommunen eller om de behandlas av någon utomstående leverantör på uppdrag av kommunen (ett så kallat personuppgiftsbiträde).

Om behandlingen sker i strid med personuppgiftslagen eller andra bestämmelser kan den personuppgiftsansvarige ställas till ansvar, oavsett om denne haft uppsåt att handla i strid med lagen eller varit oaktsam.

Personuppgiftsansvarig ansvarar bland annat för att: (uppräkningsen är inte uttömmande):

- riktlinjerna i detta styrdokument följs,
- rutiner för dataskydd upprätthålls gällande registerutdrag, rättning och gallring av personuppgifter,
- de registrerade informeras om ändamål med behandling samt sina rättigheter, när personuppgifterna erhålls,
- nya och förändrade personuppgiftsbehandlingar registreras och uppdateras i verksamhetens / bolagets registerförteckning,
- nya och förändrade personuppgiftsbehandlingar bedöms utifrån dataskyddsförordningens bestämmelser om konsekvensbedömningar och att dessa vid behov genomförs.

- försäkra sig om att verksamheten har en ändamålsenlig organisation med tillräckliga resurser och dokumenterad ansvarsfördelning,
- säkerställa att kommunens medarbetare har nödvändig kompetens för att kunna följa dataskyddslagstiftningen,
- säkerställa att det tecknas personuppgiftsbiträdesavtal med de leverantörer som behandlar personuppgifter för kommunens räkning,
- säkerställa att personuppgiftsincidenter hanteras i enlighet med dataskyddslagstiftningens krav,
- stödja dataskyddsbudet i utförandet av de uppgifter som dataskyddsförordningen föreskriver, och
- säkerställa att lämpliga tekniska och organisatoriska säkerhetsåtgärder vidtas för att skydda personuppgifter.

Informationssäkerhetsstrateg

Det ska finnas en utpekad informationssäkerhetsstrateg i kommunen. Rollen leder och samordnar kommunens övergripande arbete med informationssäkerhet och personuppgiftshantering.

Informationssäkerhetsstrategen ansvarar för att:

- ta fram och uppdatera kommunens styrande dokument inom informationssäkerhet och personuppgiftshantering.
- utveckla, besluta och förvalta kommun övergripande metoder, anvisningar och annat stödmaterial inom båda områdena,
- ge stöd till övriga roller inom informationssäkerhet och personuppgiftshantering,
- ta fram övergripande internt utbildningsmaterial och utbilda internt inom båda områdena,
- rådfråga och samråda med dataskyddsbudet för kommunens räkning,
- ansvara för omvärldsbevakning kring informationssäkerhet och personuppgiftshantering,
- stödja i uppföljning av arbetet med både områdena,
- årligen rapportera status inom informationssäkerhet till kommunfullmäktige, och
- sammankalla Informationssäkerhetsnätverket regelbundet.

Informationssäkerhetssamordnare

Varje verksamhet och bolag utser minst en lokal informationssäkerhetssamordnare med ansvar för att arbeta löpande med frågor relaterade till informationssäkerhet och personuppgiftshantering.

Rollen ska ha ett dokumenterat och av verksamhetschefen beslutat uppdrag att arbeta med informationssäkerhet och personuppgiftshantering. Uppdraget innebär bland annat att:

- är ett stöd till verksamhetens ledning kring informationssäkerhet och personuppgiftshantering,

- stödjer verksamheten i utförandet av operativa aktiviteter, exempelvis uppdatering av registerförteckning och genomförande av konsekvensbedömning (personuppgiftshantering) eller informationsklassning och riskanalyser (informationssäkerhet),
- stödja verksamheten i att uppmärksamma och åtgärda incidenter inom informationssäkerhet och personhantering,
- rådfråga och samråda med dataskyddsombudet för verksamhetens räkning,
- rapporterar status om verksamhetens arbete kring informationssäkerhet och personuppgiftshantering till verksamhetens ledning löpande samt på begäran till Informationssäkerhetsstrategen,
- deltar regelbundet i Informationssäkerhetsnätverkets arbete.

Informationssäkerhetsnätverk

I kommunen ska finnas ett informationssäkerhetsnätverk för samordning av kommunens informationssäkerhet och personuppgiftshantering. Nätverket leds av informationssäkerhetsstrateg och dataskyddsombudet. Representanter för kommunens verksamheter ska ingå i nätverket och inneha rollen informationssäkerhetssamordnare.

Nätverket ansvarar för att ta fram gemensamma mallar, arbetssätt och rutiner gällande informationssäkerhet och personuppgiftshantering. Nätverket har också till ansvar att identifiera behov för kompetensutveckling och utbildning inom informationssäkerhet och personuppgiftshantering.

Övriga chefer och medarbetare

Samtliga medarbetare har ett ansvar för att behandlingen av personuppgifter utförs på ett korrekt och lagligt sätt. Riktlinjer, rutiner och arbetsinstruktioner ska vara kända inom organisationen och det åligger varje chef att förmedla vikten av att följa gällande styrdokument och gällande lagstiftning.

Chefer har även ansvaret att agera på personuppgiftsincidenter.

Dataskyddsombud

Dataskyddsombudet är utsett av den personuppgiftsansvarige och kan representera flera personuppgiftsansvariga (nämnder/bolag). Beslut om nytt dataskyddsombud fattas enligt kommunens delegationsordning och dataskyddsombudets kontaktuppgifter ska anmälas till tillsynsmyndigheten.

Dataskyddsombudets arbetsuppgifter och ställning styrs av lagstiftning. Funktionen är självständig. Dataskyddsombudet har inget eget ansvar för att kommunen följer dataskyddslagstiftningen, det ansvaret ligger alltid hos den personuppgiftsansvarige. Ombudet har i uppdrag att bland annat granska efterlevnaden av dataskyddslagstiftningen samt att ge stöd och råd i arbetet.

Uppdraget innebär bland annat att:

- samla in information om hur verksamheten behandlar personuppgifter,

- kontrollera att verksamheten följer bestämmelser och interna styrdokument på dataskyddsområdet,
- informera, utbilda och ge råd inom verksamheten,
- ge råd vid riskanalyser och konsekvensbedömningar,
- ta emot information om misstänkt eller konstaterad personuppgiftsincident och ge råd avseende incidenten under pågående hantering,
- stödja personuppgiftsansvarig vid upprättande av personuppgiftsbiträdesavtal,
- vara kontaktperson för Integritetsskyddsmyndigheten,
- vara kontaktperson vad gäller dataskydd för de registrerade (inkl. medarbetare) inom verksamheten,
- samarbeta med Integritetsskyddsmyndigheten, till exempel vid tillsyn,
- upprätta och redovisa en årlig granskningsrapport om organisationens efterlevnad av dataskyddsförordningen, som inkluderar förslag på åtgärder,
- delta i Informationssäkerhets- och dataskyddsnätverket regelbundet.

Dataskyddsombudet ska kunna arbeta självständigt och oberoende inom organisationen och det är därför viktigt att dataskyddsombudet inte har några andra arbetsuppgifter som kan innebära en intressekonflikt med rollen som dataskyddsombud.

Grundläggande principer vid behandling av personuppgifter

I dataskyddsförordningen finns ett antal grundläggande principer som gäller för all personuppgiftsbehandling. Principerna innebär bland annat att personuppgiftsansvariga är skyldiga att se till att följande gäller för all personuppgiftsbehandling.

Barnperspektiv - Barn förtjänar ett särskilt skydd enligt dataskyddsförordningen. Information som riktar sig till barn ska vara skriven på ett tydligt och enkelt sätt.

Principen om laglighet, korrekthet och öppenhet – Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Att personuppgiftsbehandlingen är laglig innebär att behandlingen ska stödja sig på en av de 6 rättsliga grunderna som finns att tillgå:

- Rättslig förpliktelse (exempelvis bokföringslagen)
- Avtal (exempelvis anställningsavtal)
- Myndighetsutövning (exempelvis bygglov, ekonomiskt bistånd, utbildning)
- Allmänt intresse
- Intresseavvägning
- Samtycke (se även nedan).

I kommunal verksamhet används främst de rättsliga grunderna rättslig förpliktelse, uppgift av allmänt intresse eller myndighetsutövning samt avtal.

Samtycke används sällan i kommunal verksamhet eftersom samtycke måste vara en fråga om frivillig, specifik och otvetydig viljeyttring från den registrerade efter att denne ha fått information om behandlingen. I kommunal verksamhet är den registrerade ofta i beroendeställning i förhållande till kommunen varför ett samtycke inte kan anses vara frivilligt.

Om behandlingen ändå grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter. Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Att ett samtycke ska vara frivilligt kan sägas innebära att den enskilde i praktiken måste ha ett fritt val att avgöra om hans eller hennes uppgifter ska få behandlas. Den registrerade kan när som helst återkalla sitt samtycke vartefter behandling inte längre får ske.

Kommunens behandling av personuppgifter ska vara rättvis, proportionerlig och stå i rimlig relation till det syfte den tjänar. Innan behandlingen påbörjas ska en avvägning mellan kommunens egna och de registrerades intressen göras. Behandlingen ska vara förutsägbar för de registrerade och genomföras på ett öppet och tydligt sätt, utan att vilseleda eller manipulera. Det ska vara tydligt för de registrerade hur deras personuppgifter behandlas, vilken information som samlas in, varför den samlas in och hur den används. De ska också informeras om sina rättigheter, som att få felaktiga uppgifter rättade eller raderade.

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.

Uppgiftsminimering - Uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Riktighet – Uppgifterna som behandlas ska vara riktiga och uppdaterade.

Lagringsminimering - Uppgifterna får inte behandlas under en längre tid än vad som är nödvändigt.

Integritet och konfidentialitet - 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 organisatoriska, fysiska, tekniska och administrativa åtgärder.

Ansvarsskyldighet - Det är den personuppgiftsansvarige som ansvarar för att kunna visa att samtliga principer efterlevs i samtliga personuppgiftsbehandlingar. Lagring och gallring av personuppgifter ska ske i enlighet med gällande hanteringsanvisningar för respektive nämnd.

Den registrerades rättigheter

Enligt dataskyddsförordningen har den registrerade ett antal rättigheter gentemot personuppgiftsansvarig. 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 (2018:2018).

Rätt till tillgång - Den registrerade har alltid rätt att begära tillgång till de personuppgifter som behandlas och grunderna för behandlingen. Detta kallas också rätt till registerutdrag. Ett registerutdrag får aldrig skickas via e-post till den registrerade.

Rätt till rättelse - Den registrerade har rätt att få felaktiga personuppgifter rättade. Det innebär också att den registrerade har rätt att komplettera med sådana uppgifter som saknas och som är relevanta med hänsyn till ändamålet med behandlingen.

Rätt till radering - Om den registrerade begär att bli bortglömd är personuppgiftsansvarig skyldig att radera personuppgifterna i vissa särskilda fall. Rätten att bli bortglömd är dock mycket begränsad i offentlig verksamhet då det inte sällan krävs att personuppgifterna sparas för att uppfylla lagstiftningens krav på bevarande av allmänna handlingar.

Rätt till information - Den registrerade har rätt att få information om personuppgiftsbehandlingen. Generell information om den personuppgiftsbehandling som sker i kommunens verksamhet finns publicerad på kommunens externa webbplats.

Övriga rättigheter - Den registrerade har i vissa fall rätt att begära att få ut sina uppgifter i allmänt läsbart format (rätt till dataportabilitet), att begära att personuppgiftsbehandlingen begränsas (rätt till begränsning), att göra invändningar mot personuppgiftsbehandlingen (rätt till invändning) och att inte bli föremål för beslut som enbart grundas på någon form av automatiserat beslutsfattande. Den registrerade kan lämna klagomål som avser behandling av personuppgifter till personuppgiftsansvarig eller till tillsynsmyndigheten.

Konsekvensbedömning

Om en personuppgiftsbehandling sannolikt leder till hög risk för fysiska personers fri- och rättigheter ska den personuppgiftsansvarige utföra en konsekvensbedömning. Bedömningen ska göras innan en ny behandling påbörjas, vid pågående behandlingar som inte bedömts tidigare eller vid pågående där risken för den enskilde har ökat.

Syftet med bedömningen är att:

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

Ansvarig chef för den enhet eller verksamhet som initierar en ny personuppgiftsbehandling ansvarar för konsekvensbedömning görs. Dataskyddsombudet bör alltid rådfrågas vid upprättandet av en konsekvensbedömning.

Kommunen ska en upprättad mall för konsekvensbedömning som ska användas vid bedömningen.

Registerförteckning

Varje nämnd och kommunalt bolag ska enligt artikel 30 i dataskyddsförordningen föra ett register över sina behandlingar av personuppgifter. Register ska upprättas skriftligen, vara tillgängliga i elektroniskt format och hållas uppdaterade.

Mall för registerförteckning ska användas.

Ansvarig chef för den enhet eller verksamhet som initierar en ny personuppgiftsbehandling ansvarar för personuppgiftsbehandlingen tas upp i registerförteckningen.

Säkerhetsåtgärder vid personuppgiftsbehandling

Den personuppgiftsansvarige är skyldig att vidta sådana säkerhetsåtgärder som skyddar de personuppgifter som behandlas. Åtgärderna kan vara organisatoriska, fysiska, tekniska och administrativa. Åtgärderna ska vara utformade så att de ger en relevant säkerhetsnivå med hänsyn till tekniska möjligheter, kostnader, särskilda risker med behandlingen av personuppgifterna och hur känsliga personuppgifterna är i det aktuella fallet.

Säkerheten ska baseras på genomförd informationsklassning. Behandling av känsliga och integritetskänsliga personuppgifter ställer högre krav på säkerhetsåtgärder.

Personuppgiftsincident

En personuppgiftsincident är en händelse som **kan**¹ leda till oavsiktlig eller olaglig förstöring, förlust eller ändring, obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Det spelar ingen roll om det inträffade har skett oavsiktligt eller med avsikt.

Exempel på personuppgiftsincidenter:

- a) En obehörig har gjort ett intrång i ett verksamhetssystem där personuppgifter lagras
- b) Utskrift med känsliga personuppgifter har glömts kvar i en skrivare på kommunen
- c) En dator eller mobil har tappats bort och användaren haft tillgång till personuppgifter via datorn /mobilen.

En personuppgiftsincident ska rapporteras till närmaste chef och/eller dataskyddsombudet skyndsamt efter att incidenten upptäcktes. Chef gör en konsekvensbedömning i med stöd av dataskyddsombudet och beslutar om incidenter ska anmälas till Integritetsmyndigheten (IMY) Anmälan ska senast 72 timmar från det att organisationen fick vetskap om incidenten.

En personuppgiftsincident ska hanteras enligt kommunens Rutin för incidenthantering som finns på intranätet under Informationssäkerhet.

Personuppgifter i e-post

¹ Notera ordet kan. Jämför exempel a) där personuppgifter har röjts med situationen i c) där det finns risk att de kan bli röjda.

E-post innehåller alltid minst en personuppgift, e-postadressen. Det betyder att dataskyddsförordningen är tillämplig även vid e-posthantering. Precis som vid övriga behandlingar krävs det att det finns en rättslig grund som tillåter att behandling av personuppgifter får göras i e-post. Det kan till exempel vara att kontakten sker som ett led i myndighetsutövning.

En användares e-postlåda inte en lämplig permanent lagringsyta och informationen ska i stället överföras till exempelvis verksamhets-, ärendehanterings- och diariesystem.

Skicka aldrig stora mängder personuppgifter, integritetskänsliga eller känsliga personuppgifter i e-post. Filer som innehåller stora mängder personuppgifter bör inte heller kommuniceras via e-post, oavsett om det sker internt eller externt.

Personuppgifter i Microsoft365

De flesta av de personuppgifter kommunen hanterat ska i första hand hanteras och lagras i verksamhetssystem. Alla dokument, även de som innehåller personuppgifter, som lagras på M365 ska ha känslighetsetikett. Använd anvisningarna som finns under ikonerna Känslighet i exempelvis Word och Excel.

Dokument som har en känslighet över 2. Begränsad får aldrig lagras i M365.

Det är även viktigt att undvika integritetskänsliga och känsliga personuppgifter vid användning av Chatt, Teams och andra M365 funktioner och appar.

Publicering av personuppgifter på internet

Personuppgifter får endast publiceras på kommunens hemsida och på sociala medier om det finns en rättslig grund för det. Känsliga eller skyddsvärda personuppgifter får aldrig publiceras på internet.

Publicering av anställdas personuppgifter, såsom namn, befattning, telefonnummer och e-postadress till arbetet och liknande arbetsplatsrelaterade personuppgifter kan normalt publiceras utan den registrerades samtycke om publiceringen är nödvändig för att informera om kommunens verksamhet. Den rättsliga grunden för publiceringen är i sådant fall utföra uppgift av allmänt intresse. Uppgifter om familjeförhållanden, bostadsadress, telefonnummer och fritidsintressen får inte publiceras. Personuppgifter som namn och partitillhörighet som rör en förtroendevald och dennes uppdrag får normalt sett publiceras.

Publicering av bilder och film

Dataskyddsförordningen gäller även för de bilder och filmer som publiceras av kommunen på hemsida eller sociala medier och där objektet är en identifierbar person. De personer som är med på fotot ska ges information om samt ges rätt till att invända mot publiceringen.

Foto på chefer och förtroendevalda får publiceras med stöd av den rättsliga grunden allmänt intresse, om syftet med publiceringen är att informera om kommunens verksamhet. Foto på anställda i publika roller kan normalt sett också publiceras med stöd av samma rättsliga grund,

allmänt intresse. Däremot kan inte den rättsliga grunden åberopas för att publicera bilder på alla anställda, som till exempel enskilda handläggare.

Publicering av foton och filmer där övriga registrerade förekommer kan i vissa fall vara en uppgift av allmänt intresse, exempelvis om ändamålet med publiceringen är att informera om kommunens verksamhet. En bedömning måste dock göras i varje enskilt fall med hänsyn till de aktuella omständigheterna. I vissa sammanhang går det också att stödja sig på den registrerades samtycke.

Tänk på att alltid dokumentera ändamålen med personuppgiftsbehandlingen, valet av rättslig grund samt varför behandlingen är nödvändig. Foton och filmer får inte publiceras slentrianmässigt utan ska tillföra något i sammanhanget. Den registrerade ska alltid få information om att fotografering eller filmning kommer att ske och möjlighet att avstå medverkan.

Personuppgifter vid upphandling

Innan inköp av system eller tjänster i vilka personuppgifter kommer att behandlas ska beställaren kartlägga, analysera och ställa krav så att dataskyddslagstiftningen beaktas. Det ska alltid bedömas om en risk- och konsekvensbedömning ska genomföras.

Innan personuppgiftsbehandlingen påbörjas eller tekniska hjälpmedel köps in ska ändamålet med behandlingen samt den rättsliga grunden vara fastställd. Antalet uppgifter som behandlas ska inte vara fler än vad som är nödvändigt i förhållande till ändamålet.

Personuppgiftsbiträdesavtal ska alltid tecknas i de fall ett personuppgiftsbiträde anlitas.

En checklista för upphandling ska skapas och den ska inkludera aspekter kopplade till hantering av personuppgifter.

Introduktion av nyanställda

Vid introduktion av nyanställda och inhyrd personal ska information om dataskyddsförordningen ingå. Den nyanställde / inhyrda ska även få ta del av denna riktlinje.