GRUMS KOMMUN

RIKTLINJER

Datum
2023-06-07

Reviderad datum

Antagen av
KS 2023-08-31

Paragraf
§ 187

Riktlinje för informationssäkerhet och dataskydd

Innehåll

Om riktlinjer för informationssäkerhet och dataskydd

I Grums kommuns policy för informationssäkerhet och dataskydd framgår kommunens övergripande viljeinriktning för informationssäkerhet och dataskydd i kommunen.

Denna riktlinje syftar till att beskriva kommunens övergripande förhållningssätt och anvisningar för hur viljeinriktningen i policyn ska uppnås.

Definitioner av informationssäkerhet

Informationssäkerhetsarbetet i Grums kommun omfattar alla typer av information, både i text, ljud, bilder, film och så vidare. Det gäller oavsett hur informationen lagras, bearbetas eller kommuniceras.

Informationssäkerhet i Grums kommun handlar framför allt om att hindra information från att läcka ut, förvanskas och förstöras. Det handlar också om att rätt information ska finnas tillgänglig för rätt personer, och i rätt tid. Information ska inte kunna hamna i orätta händer eller missbrukas.

I Grums kommun definieras begreppen enligt följande:

- Riktighet
  innebär att kommunens verksamheter kan lita på att informationen är korrekt.
- Tillgänglighet
  innebär att kommunens verksamheter alltid ska ha tillgång till den information som krävs för att utföra sina arbetsuppgifter.
- Konfidentialitet
  innebär att endast behöriga ska kunna ta del av informationen.

Grundläggande principer

En väl utvecklad och integrerad informationssäkerhet i kommunens verksamhet bidrar till att etablera en effektiv och ändamålsenlig informationshantering. Det skapar förtroende både inom och utanför organisationen, hjälper kommunen att bygga ett skydd mot it-attacker och läckage av personuppgifter och säkerställer en säker verksamhetsstyrning. Det är också en metodik och ett systematiskt arbetssätt för att efterleva lagstiftning och löpande uppföljning.

Arbetssättet ska vara systematiskt där kommunen kontinuerligt anpassar skyddet utifrån identifierat behov och risker.

Fysiskt skydd

Fysiskt skydd av information ska vara en naturlig del i kommunens informationssäkerhetsarbete. Tekniska skydd ska utformas i enlighet med gällande lagstiftning samt följa svenska skyddsnormer och praxis. Fysiskt skydd ska i huvudsak regleras inom följande områden:

- områdesskydd
- skalskydd och säkerhetszoner
- tillträde till utrymmen
- särskilt skyddsvärda utrymmen (arkiv, datahallar, teleutrymmen etc.)
- brandskydd
- skydd av utrustning
- bevakning
- fastighetsautomation och övervakning

Klassning av information

Informationsklassning ska vara en grundläggande komponent i informationssäkerhetsarbetet. Information i Grums kommun ska klassas på ett enhetligt sätt genom en organisationsgemensam modell för informationsklassning.

Klassningsmodellen ska definiera konsekvensnivåer kopplat till de tre aspekterna konfidentialitet, riktighet och tillgänglighet så att skyddsåtgärder motsvarar informationens skyddsvärde.

Klassning av informationen ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Grums kommuns verksamheter.

Informationshanteringsplan

För att arbeta effektivt med informationssäkerhet och dataskydd ska kommunens dokumenthanteringsplaner ersättas av en kommungemensam informationshanteringsplan. I informationshanteringsplanen ska handlingstyper finnas klassade och bedömda utifrån sitt skyddsvärde, där personuppgifter är en variabel som ska ligga till grund i bedömningen.

Systemförvaltning

I Grums kommun ska informationssäkerhet vara en naturlig del i förvaltningen av kommunens system.

Alla kommunens system ska vara dokumenterade. Det ska finnas en systemförvaltarorganisation som tydligt pekar ut roller och ansvarsfördelning. Skyddsvärda system ska alltid ha förvaltningsplaner där säkerhetsåtgärder tydligt finns dokumenterade med plan för uppföljning.

Det ska finnas rutiner som säkerställer kontinuitet och drift av kommunens verksamhetskritiska system. Nyckelpersonsberoende ska undvikas i möjligaste mån.

Systemförvaltningens mål, eller åtgärder, kan uppkomma eller motiveras med exempelvis resultat från genomförda riskanalyser, revisioner, erfarenheter från inträffade incidenter eller krav i dessa riktlinjer.

Risk- och sårbarhetsanalyser

Information och personuppgifter ska skyddas med relevanta skyddsåtgärder. Med hjälp av risk- och sårbarhetsanalyser ska kommunen tillämpa ett riskbaserat förhållningsätt där skyddsåtgärder baseras på den risk som behandlingen medför för de registrerade eller efter informationens känslighet och värde för verksamheten.

Genom att risk- och sårbarhetsanalyser är en naturlig del i verksamheternas ordinarie processer samt kommunens årliga process för verksamhetsplanering, kan verksamheterna planera och budgetera för riskeliminering.

Risk- och sårbarhetsanalyser ska alltid övervägas vid:

- Vid införande av nya system som innehåller en större mängd personuppgifter eller information som vid förlust av tillgång innebär konsekvenser för verksamheten.
- Vid alla nya personuppgiftsbehandlingar där känsliga personuppgifter behandlas.
- I samband vid större verksamhetsförändringar, exempelvis organisationsförändringar.

Konsekvensbedömning

När en personuppgiftsbehandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska alltid en konsekvensbedömning göras.

Grums kommun ska kontinuerligt bedöma den risk som uppkommer vid personuppgiftsbehandlingar för att identifiera när en konsekvensbedömning ska ske.

Säkerhetsmedvetande

Grums kommun ska ha rutiner för att säkerställa att medarbetare har grundläggande kunskaper om informationssäkerhet och dataskydd.

Upphandling

För att säkerställa att upphandlade objekt får tillfredställande skyddsnivåer, ska kommunen ha organisationsövergripande rutiner där

informationssäkerhetsaspekter beaktas vid varje upphandling. Skyddsnivåerna ska motsvara informationens skyddsvärde.

Dataskyddsombud

I Grums kommun utser varje nämnd dataskyddsombud. Dataskyddsombudets uppgifter är bland annat att:

- informera och ge råd till den personuppgiftsansvarige och de anställda som behandlar personuppgifter om deras skyldigheter
- övervaka efterlevnaden av dataskyddsförordningen
- vara rådgivande vid konsekvensbedömningar
- samarbeta och vara kontaktperson för tillsynsmyndigheter
- arbeta riskbaserat och stödja organisationen med att inrikta arbetet på de eventuella problem som utgör en högre risk för dataskyddet.

Behandling av personuppgifter

När Grums kommun ska behandla personuppgifter måste de grundläggande principerna i dataskyddsförordningen alltid efterlevas:

- det ska finnas en rättslig grund i dataskyddsförordningen,
- bara personuppgifter för det specifika, särskilt angivna och berättigade ändamålet får samlas in,
- bara de personuppgifter som behövs för ändamålen får behandlas,
- personuppgifterna ska vara korrekta,
- personuppgifterna ska gallras när de inte längre finns någon rättslig grund för behandlingen,
- personuppgifterna ska skyddas, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs,
- verksamheten ska kunna visa hur dataskyddsförordningen efterlevs.

Som rättslig grund ska Grums kommun främst använda sig av rättslig förpliktelse, uppgift av allmänt intresse, myndighetsutövning eller avtal i enlighet med artikel 6 i dataskyddsförordningen.

Behandling av känsliga personuppgifter

Dataskyddsförordningen skiljer mellan vanliga personuppgifter och känsliga personuppgifter. Normalt är det förbjudet att hantera känsliga personuppgifter, men det finns tillfällen som kommunen behöver behandla känsliga personuppgifter till exempel inom hälso- och sjukvården samt socialtjänsten.

Känsliga uppgifter måste också skyddas mer än andra uppgifter. Ju känsligare uppgifter, desto större är riskerna och därmed ökar kraven på säkerhet. Känsliga personuppgifter och sekretess får bara hanteras på särskilt utpekade lagringsytor och får aldrig hanteras i system som lyder under lagstiftning från tredje land.

Personuppgiftsbiträde

Den som behandlar personuppgifter på uppdrag av annan personuppgiftsansvarig blir personuppgiftsbiträde i förhållande till den personuppgiftsansvarige. När kommunen anlitar ett personuppgiftsbiträde ska kommunen säkerställa att denne kan ge tillräckliga garantier om att upprätthålla lämplig teknisk och organisatorisk säkerhet i enlighet med gällande rätt.

Personuppgiftsbiträdesavtal

Personuppgiftsbiträdets behandling av personuppgifter ska regleras av ett personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige (ansvarige).

Grums kommun ska använda en kommungemensam mall för personuppgiftsbiträdesavtal. Av avtalet ska bland annat framgå vad behandlingen avser, dess varaktighet, art, ändamål samt typ av personuppgifter. Avtalet ska även säkerställa att biträdet endast får behandla personuppgifter i enlighet med den ansvariges instruktion och iakttar erforderlig konfidentialitet och tystnadsplikt.

I undantagsfall kan en mall för personuppgiftsbiträdesavtal tillhandahållen av leverantören användas, då ska dataskyddsombudet ska alltid konsulteras.

Information som omfattar barn

Personuppgifter om barn anses särskilt skyddsvärda i dataskyddsförordningen. Grums kommun ska säkerställa att all information som berör barn ska hanteras med extra försiktighet, att hänsyn tas till att barns personuppgifter kräver särskilt skydd att barnets rättigheter alltid är väl skyddade.

Utvärdering och uppföljning

För att säkerställa att arbetet är ändamålsenligt utformat med avsedd verkan, ska kommunen löpande utvärdera samt följa upp arbetet med informationssäkerhet och dataskydd.

För att få en överblick över händelser samt trender som kan påverka kommunens arbete med informationssäkerhet och dataskydd, ska kommunen ska arbeta aktivt med omvärldsbevakning.

Årsrapport för informationssäkerhet och dataskydd

Arbetet med informationssäkerhet och dataskydd ska årligen rapporteras till nämnden. Som personuppgiftsansvarig ska nämnden hållas uppdaterad i det arbete som förvaltningen gör inom området informationssäkerhet och dataskydd. Rapporten ska bestå av en redogörelse för hur informationssäkerhets- och dataskyddsarbetet har bedrivits under året, större incidenter och förbättringsområden samt rekommendationer för fortsatt arbete.

Vid förekommen anledning ansvarar nämnden för att besluta om åtgärder och rekommendationer som ska verkställas.

Incidenthantering

Grums kommun ska ha en rutin som säkerställer att alla informationssäkerhetsincidenter och personuppgiftsincidenter rapporteras, utreds samt åtgärdas. Alla incidenter ska dokumenteras, inbegripet omständigheterna kring incidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Syftet med utredning och dokumentation av incidenter är bland annat att synliggöra risker och vidta åtgärder mot bakgrund av inträffade händelser. Utredningarna ska vara ett underlag för verksamheterna vid prioritering och beslut om verksamhetsförändring och tillhörande styrande dokument. Det ska också vara ett underlag för ökat medvetande om vikten av incidenthantering i organisationen.

Incidenthanteringen syftar också till att minska negativ påverkan på verksamheten, stärka motståndsförmågan och förebygga att incidenter inträffar. Genom att arbeta systematiskt med incidenthantering ska kommunen skapa en bild av nuläget och ett underlag för kontinuerligt förbättringsarbete.

Ledning och ansvar

Nämnd

Varje nämnd i Grums kommun är personuppgiftsansvarig. Det innebär att nämnden ansvarar för all behandling av personuppgifter, även om nämnden inte har bett om den eller känner till den. Om en medarbetare som på eget initiativ samlar in eller lämnar ut information i strid med lagstiftningen, är det nämndens ansvar även om det finns tydliga riktlinjer som medarbetaren brutit mot.

Konkret innebär personuppgiftansvaret att nämnden är ytterst ansvarig för att:

- dataskyddsförordningens principer och krav efterlevs i alla stadier av kommunens av personuppgiftsbehandlingar
- besluta om vad principerna i dataskyddsförordningen innebär i praktiken och hur de ska förverkligas i Grums kommun
- kommunen dokumenterar att principerna och kraven efterlevs
- verksamheterna har de resurser som krävs för att uppfylla dataskyddsförordningen och kommunfullmäktiges målsättning för informationssäkerhet.

Varje nämnd har även det yttersta ansvaret för kommunens arbete med informationssäkerhet.

Förvaltningsorganisationens ansvar

Ansvaret för informationssäkerhet och dataskydd följer ordinarie verksamhetsansvar. Detta gäller från kommunledning till enskild medarbetare och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten och dataskyddet inom det verksamhetsområdet.

Sektorchef

Sektorchef är ansvarig för det övergripande arbetet med informationssäkerhet och dataskydd inom sektorn. Sektorchef ansvarar bland annat för att:

- verksamheterna har de förutsättningar som krävs för efterlevnad av och implementering av styrdokument som reglerar kommunens informationssäkerhets- och dataskyddsarbete
- säkerställa att frågorna ges utrymme i budgetsammanhang och vid verksamhetsplanering
- det tecknas personuppgiftsbiträdesavtal för avtal som omfattar flera verksamhetsområden eller sektorer.

Chef

Eftersom ansvaret för dataskydd och informationssäkerhet följer ordinarie verksamhetsansvar, är varje chef ansvarig för sin verksamhets informationssäkerhet och dataskydd.

Det är i verksamheterna som den största kunskapen finns, om hur känslig och kritisk informationsmängderna är, och därmed informationens skyddsvärde och vilka skyddsåtgärder som krävs.

Det innebär att varje chef är informationsägare och ansvarar för sin verksamhets efterlevnad av dataskyddsförordningen. Bland annat genom att:

- **Verksamhetens informationssäkerhet uppfyller tillfredsställande nivå**
  Verksamhetens informationstillgångar ska finns kartlagda och klassade. Därigenom ska informationen förses med tillfredställande skyddsnivåer.
- **Personuppgiftsbehandlingar dokumenteras i kommunens registerförteckning**
  Alla personuppgiftsbehandlingar ska finnas dokumenterade i kommunens registerförteckning.
- **Upprätthålla verksamhetsspecifika rutiner**
  För att efterleva dataskyddsförordningen och upprätthålla en tillräcklig nivå av informationssäkerhet behöver varje verksamhet ha egna rutiner för att till exempel hålla registerförteckningen uppdaterad, radera och gallra information och behörighetstilldelning etc.
- **Incidenter rapporteras och utreds**
  När en incident uppstår i verksamheten, ska den rapporteras och utredas. Chefer ansvarar även för att återställa verksamheten och vidta lämpliga åtgärder för att minska incidentens påverkan på personuppgifter eller annan information. I ansvaret ingår också att arbeta förebyggande för att motverka incidenter.
- **Ansvara för risk- och sårbarhetsanalyser och konsekvensbedömningar**
  Att risk- och sårbarhetsanalyser görs i enlighet med kommunövergripande rutiner samt att konsekvensbedömningar görs när en personuppgiftsbehandling sannolikt leder till en hög risk för personers rättigheter och friheter.
- **Personuppgiftsbiträdesavtal**
  För de avtal som upprättas inom verksamhetsområdet, ansvarar undertecknande chef för att personuppgiftsbiträdesavtal upprättas mellan kommunen och leverantören.
- **Att personalen har de kunskaper som krävs**
  Utifrån arbetsuppgifter och ansvar varierar personalens behov av kunskap inom området och varje medarbetare behöver ha rätt kunskapsnivå för sin roll.
- **Verksamheten följer kommunövergripande rutiner och riktlinjer**
  Till exempel att risk- och sårbarhetsanalyser görs när det behövs, att alla medarbetare känner igen en personuppgiftsincident och rapporterar den enligt rutin och att personuppgiftsbiträdesavtal alltid finns vid biträdessituationer.

Medarbetare

Alla medarbetare i Grums kommun har ett ansvar för kommunens informationssäkerhet och dataskydd genom att följa kommunövergripande rutiner och riktlinjer samt verksamhetsspecifika rutiner. Medarbetare bidrar till att upprätthålla informationssäkerhet och efterlevandet av dataskyddsförordningen genom att:

- **Hantera kommunens information ansvarsfullt**
  Alla medarbetare ska vara noga med att inga obehöriga kan ta del av informationen som hanteras, att information förvaras på angivna ställen och att verksamhetens rutiner efterlevs. Medarbetare i Grums kommun ska vara medvetna om att information kan vara både muntlig, skriftlig och digital.
- **Följa kommunens rutiner och anvisningar**
  Grums kommun har ett antal rutiner och anvisningar som kan variera mellan olika verksamheter. Medarbetare ska utgå från vad som gäller för sin verksamhet.
- **Rapportera incidenter**
  Alla medarbetare ska uppmärksamma och rapportera misstänkta incidenter. De ska vara medvetna om att incidenter kan påverka säkerheten för kommunens information och följa kommunens rutin för incidentrapportering.