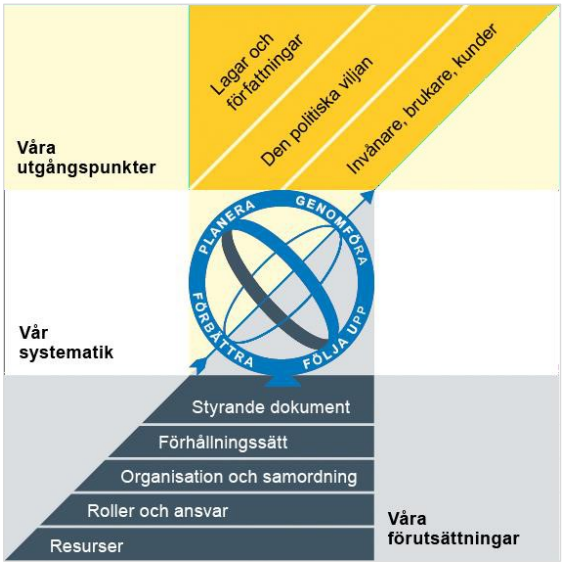
Göteborgs Stad

Äldre samt vård- och omsorgsförvaltningens rutin för hantering av personuppgiftsincidenter

Reglerande styrande dokument

- Policy
- Riktlinje
- Regel
- Anvisning
- ► **Rutin**
- Instruktion

Göteborgs Stads styrsystem



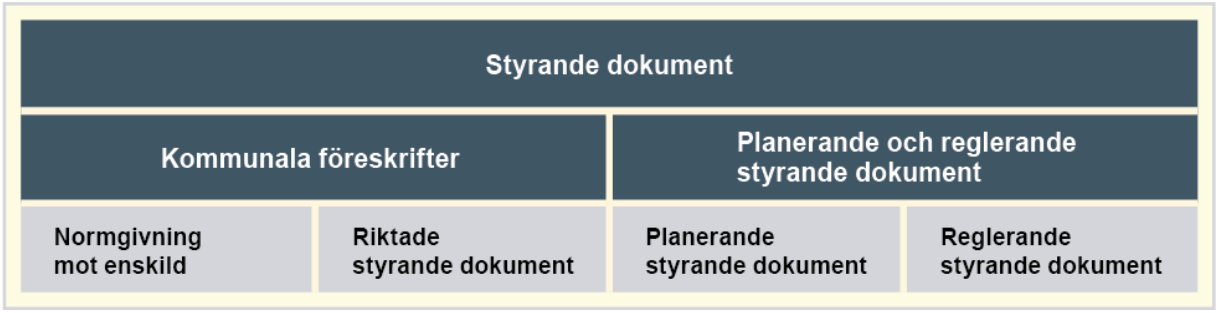
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Säkerhetschef	Äldre samt vård- och omsorgsförvaltningen	AVO-2024-02130	2024-12-05
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Rutin	Tills vidare	2024-11-28	Dataskyddskontakt

Bilagor:

Innehåll

Inledning

Syftet med denna rutin

Denna rutin beskriver hur förvaltningen hanterar personuppgiftsincidenter.

Vem omfattas av rutin

Denna rutin gäller tills vidare för chefer och medarbetare i förvaltningen.

Bakgrund

Varje personuppgiftsansvarig (PuA), tillika nämnden, har skyldighet enligt EU:s dataskyddsförordning att hantera och dokumentera personuppgiftsincidenter. Det gäller oavsett om personuppgiftsincidenten föranleder en anmälan till tillsynsmyndigheten, Integritetsskyddsmyndigheten (IMY), eller om den hanteras internt i förvaltningen.

I äldre samt vård- och omsorgsförvaltningen finns det utsedda dataskyddskontakter som är förvaltningens kontaktpersoner för frågor som rör incidenter och har delegation på att anmäla personuppgiftsincidenter i det fall detta krävs.

Koppling till andra styrande dokument

Styrande dokument	Koppling till denna rutin
Äldre samt vård- och omsorgsförvaltningens rutin för informationssäkerhet	Personuppgiftsincidenter utgör en del av området informationssäkerhet: Äldre samt vård- och omsorgsförvaltningens rutin för informationssäkerhet

Rutin för hantering av personuppgiftsincidenter

Vad är en personuppgiftsincident?

En personuppgiftsincident är en säkerhetshändelse som har påverkat sekretessen, integriteten eller tillgängligheten till personuppgifter. En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har:

- Gått förlorade eller ändrats
- Röjts för någon obehörig
- Förstörts

Det spelar ingen roll om incidenten inträffat avsiktligt eller oavsiktligt – båda fallen betraktas som en personuppgiftsincident som kan innebära risker för den registrerade. Information om en personuppgiftsincident kan nå förvaltningen från olika källor, exempelvis via en leverantör, systemförvaltare, en anställd eller medborgare.

Exempel på personuppgiftsincidenter:

- Känsliga personuppgifter skickas av misstag till fel mottagare eller utan kryptering
- Uppgifter som är skyddade av sekretess publiceras av misstag i offentliga handlingar
- En anställd får obehörig åtkomst till personuppgifter eftersom behörigheter till ett verksamhetssystem är felaktiga
- Mobila enheter som innehåller känsliga personuppgifter förloras eller stjäls.
- Personuppgifterna raderas av misstag som kan försvåra för förvaltningens tjänster och handläggning av ärenden.

Det är viktigt att lära sig identifiera personuppgiftsincidenter för att agera snabbt. Mer om grunderna i dataskyddsförordningen och om personuppgiftsincidenter lär du dig på Dataskydd på jobbet.

Så rapporterar du en personuppgiftsincident

Samtliga medarbetare och chefer som upptäcker eller misstänker en personuppgiftsincident ska rapportera till förvaltningens dataskyddskontakt Incident - Äldre samt vård omsorgsförvaltningenn

Beskriv händelsen detaljerad och besvara följande frågor vid anmälan:

- Vad är orsaken till incidenten?
- Hur många personer är drabbade av incidenten (gör en uppskattning om du inte säkert vet)?
- Vilka personuppgifter är berörda?
- Vilken känslighet har uppgifterna?
- Hur många personuppgifter gäller det?

Tänk på att anmäla en gång för mycket än en för liten. Du kan också ställa frågor via dataskyddskontakt@aldrevardomsorg.goteborg.se där du kan få hjälp att avgöra om en händelse också är en personuppgiftsincident.

Bedöm riskerna för de registrerade

För att snabbt kunna hantera, åtgärda och dokumentera personuppgiftsincidenter är det avgörande att processen sker skyndsamt och systematiskt. Ansvarig chef, eller en av chefen utsedd medarbetare, ska tillsammans med dataskyddskontakten och andra relevanta funktioner genomföra en noggrann riskbedömning. Denna bedömning måste åtminstone omfatta följande:

- Vilka risker har incidenten medfört för den registrerade?
- Vilka negativa konsekvenser kan incidenten ha för den registrerade?
- Hur sannolikt är det att konsekvenserna inträffar?
- Hur allvarlig bedöms incidenten vara?
- Vad kan vi göra för att mildra incidenten?
- Vad kan vi göra för att säkerställa att denna incident inte händer en gång till?

Riskbedömningen ska dokumenteras noggrant och användas som underlag för att avgöra om incidenten är anmälningspliktig till Integritetsskyddsmyndigheten (IMY).

Dataskyddsombud:

Förvaltningens dataskyddskontakt rådgör vid behov med dataskyddsombudet (DSO) som hjälper till med att utreda om händelsen utgör en incident, om den är anmälningspliktig till Integritetsskyddsmyndigheten (IMY) och om den registrerade måste informeras. Förvaltningens dataskyddskontakter har ansvar för att hålla dataskyddsombudet informerad och involverad i de fall detta krävs.

Anmälan till Integritetsskyddsmyndigheten

Anmälningar till Integritetsskyddsmyndigheten görs digitalt av dataskyddskontakten och dokumenteras i förvaltningens diarium som ett delegationsbeslut. Dataskyddskontakten ansvarar för att anmäla personuppgiftsincidenten till IMY inom 72 timmar efter att den har upptäckts.

Information till den registrerade

Behovet av att informera de registrerade avgörs utifrån riskanalysen. Om risken är hög måste de personer som drabbats informeras utan onödigt dröjsmål, vilket är chefens ansvar. Informationen ska vara tydlig och proaktiv för att upprätthålla förtroendet och hjälpa de registrerade att skydda sina rättigheter. Rådgör med dataskyddskontakten.

Information till de registrerade ska inkludera:

- Orsak till incidenten, beskriv på ett tydligt och begripligt sätt vad som hänt.
- Åtgärder som vidtagits eller planeras för att hantera incidenten.
- Vilka insatser förvaltningen har gjort för att mildra negativa effekter.
- Sannolika konsekvenser av de inträffade och råd för att minimera skadan.
- Kontaktuppgifter till ansvariga personer, DSO och/eller dataskyddskontakten för mer information

Vid större incidenter eller när fler förvaltningar berörs bör Kommunikationsenheten involveras för att ge råd om lämpliga informationskanaler och metoder. Kommunikationsenheten kan även bidra med att klarspråka informationen för att säkerställa att den är tydlig och lättförståelig.

Om ingen hög risk bedöms föreligga behöver de registrerade inte informeras, men beslutet ska dokumenteras i utredningen. Det är viktigt att undvika att avslöja detaljer som kan äventyra informationssäkerheten för verksamheten.

Dokumentation av personuppgiftsincidenter

För att förvaltningen ska upprätthålla ett proaktivt arbete och visa på regelefterlevnad så ska alla personuppgiftsincidenter dokumenteras, även incidenter som inte måste anmälas till IMY. Dokumentationen som upprättas ska alltid diarieföras.

Avrapportering av personuppgiftsincidenter

Dataskyddskontakten ska regelbundet rapportera inträffade personuppgiftsincidenter till följande funktioner:

- Dataskyddsombudet
- Förvaltningsledningen
- Informationsägare (verksamhetsansvarig)
- Säkerhetschef

Beroende på vad som har inträffat ska även andra funktioner som har en central roll i anmälan informeras, dessa kan vara IT, Intraservice osv. Den berörda avdelningen ansvarar för att uppföljande åtgärder genomförs, och dessa ska bedömas tillsammans med dataskyddskontakten.

Allvarliga incidenter ska omedelbart rapporteras till förvaltningsdirektören, stabschef för dataskyddsfrågor, säkerhetschefen och berörda informationsägare.

Kontaktuppgifter

Frågor om incidenter, kontakta förvaltningens dataskyddskontakter via e-post: dataskyddskontakt@aldrevardomsorg.goteborg.se