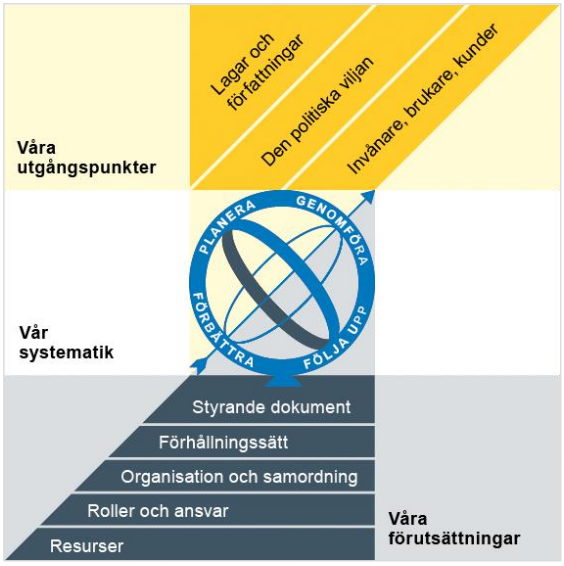
Göteborgs Stad

Äldre samt vård- och omsorgsförvaltningens rutin för hantering av personuppgiftsincidenter

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



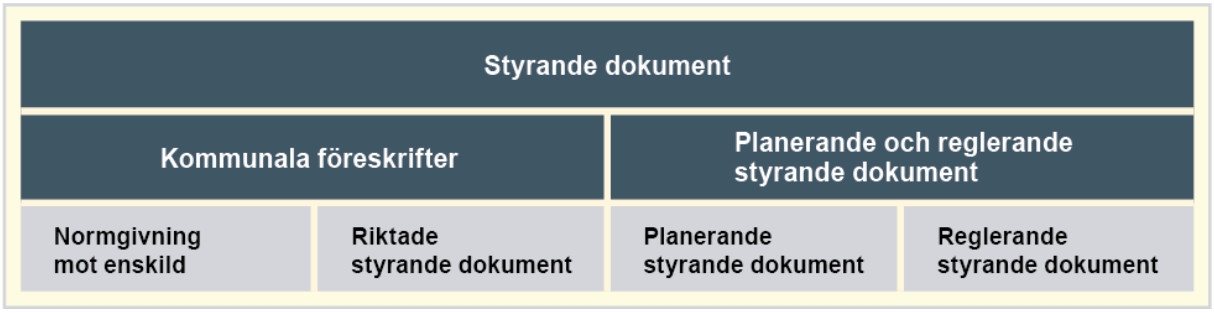
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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	160-1391/21	2021-09-22
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Rutin	Tillsvidare	2021-09-22	Dataskyddskontakt

Bilagor:

Innehåll

Inledning

Syftet med denna rutin

Denna rutin beskriver hur förvaltningen hanterar personuppgiftsincidenter.

Vem omfattas av rutin

Denna rutin gäller tillsvidare 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.

Stödjande dokument

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:

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

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det en personuppgiftsincident.

Exempel på personuppgiftsincidenter

- Någon obehörig har fått tillgång till personuppgifterna, till exempel om personuppgifter har skickats till en mottagare som inte skulle ha uppgifterna.
- Datorer som innehåller personuppgifter har förlorats eller stulits.
- Någon har ändrat personuppgifter utan tillstånd.
- Personuppgifterna är inte tillgängliga för den som behöver dem och det leder till negativa effekter för de registrerade personerna.

Information om att en personuppgiftsincident har skett kan komma till förvaltningens kännedom på flera olika sätt. Till exempel från en leverantör, systemförvaltare, en anställd eller medborgare. Vid misstanke att en personuppgiftsincident har inträffat ska förvaltningen omedelbart påbörja en utredning av händelsen.

När en personuppgiftsincident kommer in

Samtliga händelser som misstänks vara en personuppgiftsincident ska rapporteras in till förvaltningens dataskyddskontakter via dataskyddskontakt@aldrevardomsorg.goteborg.se

När en anmälan om en personuppgiftsincident kommer in till förvaltningens dataskyddskontakter sammankallas den organisation som förvaltningen har utsett för ändamålet. Dataskyddskontakterna gör en bedömning om ärendet innehåller personuppgifter och faller under Dataskyddsförordningen. Om ja, går ärendet vidare till en riskbedömning.

Frågor att besvara i det första skedet:

- Berör detta personuppgifter?
- Hur allvarlig bedöms incidenten vara?
- Är det en personuppgiftsincident?

En riskbedömning ska genomföras när Dataskyddskontakten konstaterat att en personuppgiftsincident skett. Dataskyddsombudet (DSO) hjälper till med att utreda om

händelsen utgör en incident, om den är anmälningspliktig och om den enskilda måste informeras. Riskbedömningen avgör om incidenten ska anmälas till Integritetsskyddsmyndigheten, detta gäller för personuppgiftsincidenter enligt Dataskyddsförordningen eller om incidenten ska rapporteras internt i förvaltningen.

I riskbedömningen ska följande frågor besvaras:

- Vilka konsekvenser kan incidenten ha för verksamheten?
- Vilka konsekvenser kan incidenten ha för den registrerade?
- Hur allvarlig bedöms incidenten vara?
- Vad kan vi göra för att säkerställa att denna incident inte händer en gång till?

Dokumentation av personuppgiftsincidenter

För att förvaltningen ska upprätthålla ett proaktivt arbete så ska alla personuppgiftsincidenter dokumenteras, även incidenter som inte måste anmälas till Integritetsskyddsmyndigheten (IMY) ska dokumenteras. Dokumentationen som upprättas ska alltid diarieföras oavsett om den anmäls till IMY eller inte.

Anmälningar till Integritetsskyddsmyndigheten

Anmälningar till Integritetsskyddsmyndigheten dokumenteras i förvaltningens diarium Dataskyddskontakterna ansvarar för att rapportera inom 72 timmar efter att personuppgiftsincidenten har upptäckts.

Interna personuppgiftsincidenter

Interna personuppgifter dokumenteras och diarieförs även om de inte anmäls.

Avrapportering av personuppgiftsincidenter

Dataskyddskontakterna ska på årsbasis eller förekommen anledning rapportera om inträffade personuppgiftsincidenter till följande funktioner:

- Dataskyddsombudet
- Förvaltningsledningen
- Informationsägare (verksamhetsansvarig)
- Säkerhetschef

Personuppgifter av allvarligare karaktär ska omedelbart rapporteras till förvaltningsdirektör, säkerhetschef och berörda informationsägare. Beroende på vad som har inträffat ska även andra funktioner som har en central roll i anmälan informeras, dessa kan vara IT, Intraservice etc. Det är avdelningen som berörs av incidenten som ansvarar för att åtgärderna vidtas. Åtgärder vara anmälda och godkända av dataskyddskontakten.

I samband med den årliga säkerhetsrapporten till nämnden ska sammanställning av årets personuppgiftsincidenter rapporteras.

Förvaltningens dataskyddskontakter har ansvar för att hålla dataskyddsombudet informerad och involverad i de fall detta krävs.

Kontaktuppgifter

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