

Förvaltningen för funktionsstöds rutin för hantering och anmälan av personuppgiftsincident

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.

Styrande dokument			
Kommunala föreskrifter		Planerande och reglerande styrande dokument	
Normgivning mot enskild	Riktade styrande dokument	Planerande styrande dokument	Reglerande styrande dokument

Beslutad av: AC Stab, kommunikation och säkerhet	Gäller för: Förvaltningen för funktionsstöd	Diarienummer: [Nummer]	Datum och paragraf för beslutet: 2023-11-16
Dokumentsort: Rutin	Giltighetstid: 2023-11-15 - tv	Senast reviderad: 2023-11-15	Dokumentansvarig: AC Stab, kommunikation och säkerhet

Bilagor:
Inga

Innehåll

Inledning	4
Syftet med denna rutin	4
Vem omfattas av rutinen	4
Bakgrund	4
Koppling till andra styrande dokument	4
Stödjande dokument	5
Rutin	6
Vad ska du göra när du misstänker att en personuppgiftsincident inträffat?	8
Uppföljning och efterföljande åtgärder	8
Avrapportering av personuppgiftsincidenter	9

Inledning

Syftet med denna rutin

Denna rutin beskriver hur nämnden för funktionsstöd hanterar personuppgiftsincidenter.

Vem omfattas av rutinen

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

Bakgrund

Varje personuppgiftsansvarig, 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 nämnden för funktionsstöd finns det utsedda dataskyddskontakter som är nämndens kontaktpersoner för frågor som rör incidenter och har delegation på att anmäla personuppgiftsincidenter i det fall detta krävs.

Koppling till andra styrande dokument

Följande styrande dokument har koppling till denna rutin:

Styrande dokument	Koppling till denna rutin
Göteborgs Stads riktlinje för informationssäkerhet. Beslutad av kommunfullmäktige.	Personuppgiftsincidenter utgör en del av området informationssäkerhet. Denna rutin konkretiserar nämndens ansvar för att personuppgiftsincidenter, där anmälningsskyldighet finns enligt lag eller förordning, anmäls till ansvarig myndighet.
Stödfunktionernas gemensamma servicedeklaration. Beslutad av samtliga avdelningschefer på förvaltningen för funktionsstöd.	Servicedeklarationen fastställer ansvarsfördelningen vid personuppgiftsincidenter.
Delegationsordningen beslutad av nämnden för funktionsstöd.	Delegationsordningen fastställer vem som har delegering att fatta beslut om anmälan av personuppgiftsincident till Integritetsskyddsmyndigheten vid personuppgiftsincidenter

Stödande dokument

Webbaserat formulär för [rapportering av personuppgiftsincidenter](#) inom förvaltningen för funktionsstöd.

Fördjupad kunskap om [dataskyddsförordningen, GDPR och personuppgiftshantering på Intranätet](#)

[IMYs beskrivning om vad som är en personuppgiftsincident](#)

Rutin

Vad är en personuppgiftsincident

En personuppgiftsincident är enligt dataskyddsförordningen en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

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

Exempel på incidenter

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. Det kan till exempel vara att:

- En obehörig part får tillgång till personuppgifter, till exempel om någon skickar personuppgifter till en mottagare som inte ska ha dem.
- Datorer som innehåller personuppgifter förloras eller stjäls.
- Någon ändrar personuppgifter utan tillstånd.
- Personuppgifter är inte längre tillgängliga för den som behöver dem och det leder till negativa konsekvenser för de registrerade.

Vid misstanke att en personuppgiftsincident har inträffat ska förvaltningen omedelbart påbörja en utredning av händelsen.

De registrerade kan drabbas av allvarliga konsekvenser

En personuppgiftsincident kan innebära risker för registrerade personers fri- och rättigheter och kan få allvarliga konsekvenser till exempel:

- ekonomisk skada
- diskriminering
- identitetsstöld
- bedrägeri
- skadlig ryktesspridning

Vissa personuppgiftsincidenter måste anmälas till Integritetsskyddsmyndigheten (IMY)

När det har skett en personuppgiftsincident måste förvaltningen så snabbt som möjligt göra en bedömning av de potentiella negativa konsekvenserna för de registrerade, baserat på hur allvarliga eller väsentliga dessa är och hur troligt det är att effekterna kan inträffa.

Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerade måste vi anmäla incidenten till IMY. Anmälan ska göras inom 72 timmar efter det att incidenten upptäcktes. Anmälningar till IMY dokumenteras i förvaltningens diarium.

En personuppgiftsincident som inte hanteras på ett lämpligt sätt kan påverka tilltron till den organisation som behandlar personuppgifter. Den kan också leda till att IMY genom tillsyn kan döma ut sanktionsavgifter.

Dataskyddskontakter på förvaltningen för funktionsstöd

På förvaltningen för funktionsstöd sitter dataskyddskontakterna. De kan hjälpa till med anmälningar och bedömningar av personuppgiftsincidenter, rådgivning kring dataskyddsfrågor, konsekvensbedömningar och information.

För att förvaltningen ska upprätthålla ett proaktivt arbete så ska alla personuppgiftsincidenter dokumenteras, även de som inte måste anmälas till Integritetsskyddsmyndigheten. Dessa dokumenteras i systemstödet Draftit.

Kontakta dataskyddskontakterna via dataskyddskontakt@funktionsstod.goteborg.se

Läs mer om personuppgifter och våra dataskyddskontakter på [Intranätet](#).

Dataskyddsombud

Nämnden har ett utsett dataskyddsombud som är placerad på Intraservice.

Dataskyddsombudet informerar och ger råd om skyldigheter i förhållande till dataskyddsförordningen samt ska övervaka efterlevnaden av förordningen.

Dataskyddsombudet ska fungera som kontaktpunkt i förhållande till tillsynsmyndigheten, Integritetsskyddsmyndigheten.

Vårt dataskyddsombud når du på dso@intraservice.goteborg.se

Vad ska du göra när du misstänker att en personuppgiftsincident inträffat?

1. Rapportera till förvaltningens Dataskyddskontakt, så fort du misstänker att en personuppgiftsincident inträffat. Via [denna](#) länk till Intranätet hittar du information om hur du gör. Via länken ovan fyller du i en mall i systemet Drafit kring vad som inträffat.
2. Dataskyddskontakten gör sedan en bedömning av incidenten och kommer vid behov att kontakta dig för att få en bättre förståelse kring incidenten, alternativt stämna av åtgärder.
3. Om dataskyddskontakten bedömer att incidenten ska anmälas till IMY, så ansvarar dataskyddskontakten för att anmäla. Dataskyddskontakten anmäler personuppgiftsincidenten via IMYs e-tjänst som riktar sig till personuppgiftsansvariga organisationer.
4. Dataskyddskontakten anmäler även till nämnden att ett delegationsbeslut tagits angående anmälan om personuppgiftsincident till IMY.
5. Om bedömning görs att den registrerade ska informeras om incidenten ansvarar chef för att det görs.
6. Om åtgärder behöver vidtas för att undvika liknande incidenter framöver ansvarar chef för det, med stöd av dataskyddskontakten.

Uppföljning och efterföljande åtgärder

Uppföljning av personuppgiftsincidenten dokumenteras i systemstödet Drafit.

Uppföljningen syftar till att minimera riskerna för att liknande incidenter inträffar i framtiden och för att minimera effekterna av det inträffade. Uppföljning ska göras kontinuerligt och i samband med den årliga säkerhetsrapporten till personuppgiftsansvarig.

I säkerhetsrapporten gör dataskyddskontakten en sammanställning av årets personuppgiftsincidenter samt en utvärdering och analys. Sammanställningen överlämnas även till ansvarig chef, för att användas i förbättringsarbetet på enheten.

- Chef ansvarar för att personuppgiftsincidenten följs upp. Dataskyddskontakt finns att tillgå som stöd.
- DSO kan ge råd i frågor om uppföljning.
- Annan anställd kan kopplas in för att ge information som är nödvändig för uppföljningen.

Avrapportering av personuppgiftsincidenter

Personuppgiftsincidenter av allvarigare karaktär rapporteras omedelbart till IMY och förvaltningsdirektör. Den personuppgiftsansvarige informeras vid nästkommande sammanträde. 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 enheten som berörs av incidenten som ansvarar för att åtgärder vidtas. Åtgärder ska meddelas till dataskyddskontakt och dokumenteras i systemstödet Draftit.