1. Rapportera personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks.

När verksamheten uppmärksammar eller misstänker att det har skett en personuppgiftincident, ska incidenten rapporteras internt i stadens e-tjänst som nås via intranätet. Alla personuppgiftsincidenter ska rapporteras internt, även de som eventuellt ska anmälas till Integritetsskyddsmyndigheten (se nedan).

En personuppgiftsincident kan vara allt från en liten enstaka händelse till en väldigt omfattande incident. Oavsett hur allvarlig ni bedömer att incidenten är så är det viktigt att den rapporteras så att personuppgiftsincidenten dokumenteras.

1.1 Exempel på personuppgiftsincidenter

En personuppgiftsincident kan vara av olika slag och exempelvis handla om att personuppgifter obehörigen röjs, förstörs eller att de inte längre är tillgängliga. Nedan ges några praktiska exempel på vad som skulle kunna vara en personuppgiftsincident.

1. Oavsiktlig eller olaglig förstöring av personuppgift

- Någon raderar oavsiktligt eller olagligt ett register med personuppgifter
- En ”ransomware”-attack har medfört att personuppgifter har krypterats så att de inte längre går att läsa.

2. Förlust av personuppgift

- Någon tappar ett USB-minne med personuppgifter på bussen.
- Någon skickar extern e-post med personuppgifter till fel mottagare.
- Någon sparar ett dokument med personuppgifter i fel mapp på G så att obehöriga kan läsa handlingarna.
- Ett strömavbrott orsakar driftstopp i ett IT-stöd innehållande. personuppgifter och det leder till negativa effekter för de personer som är registrerade.

3. Obehörig ändring av personuppgift

- Någon loggar obehörigen in i ett IT-stöd och ändrar medicinering för en patient inom hemvården.
- Någon ändrar omedvetet lönen för flera av stadens medarbetare.

4. Obehörigt röjande av personuppgift

- En lärare skickar e-post till fel vårdnadshavare och e-posten innehåller personuppgifter.
- En lista med medarbetare som är sjukskrivna publiceras på den externa webben.
- En medarbetare lägger ut namn och personnummer på en patient på Facebook.

5. Obehörig åtkomst

- Någon stjäl en medarbetares inloggningsuppgifter, exempelvis genom en phishing-attack, och får på så sätt obehörigen tillgång till personuppgifter.
- Staden utsätts för ett antagonistiskt angrepp genom exempelvis hacking eller malware.
- Någon obehörig bereder sig tillgång till ett låst arkivskåp med handlingar innehållande personuppgifter.
- Behörigheter i ett IT-system tilldelas felaktigt eller för generellt vilket gör att obehöriga personer i verksamheten får tillgång till personuppgifter
- Det upptäcks att personuppgifter har funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning.

1.2 Hur ska rapportering ske?

Ansvarig nämnd och dess förvaltning ansvarar för att personuppgiftsincidenter rapporteras i e-tjänsten samt i förekommande fall till Integritetsskyddsmyndigheten. Det är upp till varje nämnd och dess förvaltning att bestämma vem/vilka som ska rapportera internt i e-tjänsten.

Rapportering internt sker genom att verksamheten besvarar de frågor som finns i stadens e-tjänst. Det går att förbereda sig i förväg genom att den som ska rapportera går igenom frågorna i tjänsten, se bilaga 6:1.

Den rapport som genereras i e-tjänsten skickas till förvaltningens registrator, som skickar rapporten vidare till den person som har utsetts som mottagare för rapporten på förvaltningen.

Den rapport som genereras i stadens e-tjänst kan användas som ett underlag inför en eventuell anmälan till Integritetsskyddsmyndigheten.

1.3 När ska en incident anmälas till Integritetsskyddsmyndigheten?

En personuppgiftsincident som rapporteras internt, ska i vissa fall även anmälas till Integritetsskyddsmyndigheten. Det ska ske i alla fall förutom om det är osannolikt att incidenten
kommer innebära risker för de registrerade.

En anmälan till Integritetsskyddsmyndigheten ska göras inom 72 timmar från den tidpunkt då någon i staden fick kännedom om incidenten. Det är därför mycket viktigt att incidenten rapporteras omgående i stadens e-tjänst.

Faktorer av central betydelse för bedömning av personuppgiftsincidentens allvarlighet är bland annat vilken typ av personuppgifter det gäller, hur många personuppgifter det gäller, vilka personkategorier som berörs, hur många registrerade som berörs och hur sannolikt det är att personuppgifterna kommit till obehörigas kännedom.

En personuppgiftsincident som rör behandling av personuppgifter som klassas som känsliga är i sin natur mer allvarlig än en behandling av personuppgifter där bara namn framkommer. Känsliga personuppgifter är ras eller etniskt ursprung, medlemskap i fackförening, sexualliv, hälsa, politiska åsikter, sexuell läggning, religiös/filosofisk övertygelse, biometriska uppgifter och genetiska uppgifter.

Ju högre sannolikheten är för att personuppgifterna kommit till obehörigas kännedom desto allvarligare är personuppgiftsincidenten.

Risker för fysiska personers rättigheter och friheter kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel på detta är diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust, brott mot sekretess eller tystnadsplikt

Vid osäkerhet av om en incident ska anmälas, kan verksamheten samråda med stadsjuridiska enheten eller nämndens dataskyddsombud. Verksamheten och stadsjuridiska enheten eller dataskyddsombudet tar gemensamt ställning till om incidenten ska anmälas till Integritetsskyddsmyndigheten.

För mer information om hur anmälan ska göras, se Integritetsskyddsmyndighetens webbplats.

2. Information till enskild

Om en personuppgiftsincident medför en hög risk för de registrerade, t.ex. om det finns risk för id-stöld eller bedrägeri, behöver verksamheten informera de enskilda som berörs av incidenten.

Informationen ska meddelas till den registrerade utan onödigt dröjsmål. Undantag från informationsskyldigheten föreligger om:

1. Tekniska eller organisatoriska skyddsåtgärder har tillämpats på de berörda personuppgifterna (exempelvis om de förlorade personuppgifterna är krypterade).

2. Ytterligare åtgärder är vidtagna som garanterar att den höga risken för att registrerades rättigheter och friheter kränks sannolikt inte längre kommer att förverkligas.

3. Det skulle innebära oproportionerlig ansträngning att rapportera till alla de registrerade, men då måste istället allmänheten informeras eller annan liknande åtgärd vidtas så att de registrerade ändå får tillgång till informationen.

Om det bedöms att den personuppgiftsansvarige måste lämna information om personuppgiftsincidenten till den registrerade ska följande information lämnas enligt dataskyddsförordningen.

1. En beskrivning av omständigheterna kring personuppgiftsincidenten.
2. Förmedling av namn och kontaktuppgifter till Dataskyddsombudet eller namn på annan kontaktperson/er som kan lämna ytterligare relevant information.
3. En beskrivning av sannolika konsekvenser av personuppgiftsincidenten.
4. En beskrivning av de åtgärder som vidtagits av personuppgiftsansvarig för att hantera personuppgiftsincidenten samt vidtagna åtgärder för att mildra möjliga negativa effekter till följd av personuppgiftsincidenten.

Samråd kan vid behov ske med stadsjuridiska enheten eller nämndens dataskyddsombud.

3. Information när nämnden är personuppgiftsbiträde åt annan

För det fall nämnden är personuppgiftsbiträde till en annan aktör, som i sin tur är personuppgiftsansvarig för en viss personuppgiftsbehandling, är nämnden skyldig att informera den personuppgiftsansvarige om personuppgiftsincidenter som skett i nämndens verksamhet och som påverkar de personuppgifter som nämnden behandlar för den personuppgiftsansvariges räkning. Den personuppgiftsansvarige ska i dessa fall informeras utan onödigt dröjsmål efter att någon i nämndens organisation har fått vetskap om incidenten.