ROBERTSFORS KOMMUN

Rutin anmälan av större personuppgiftsincident eller it-incident till Datainspektionen eller MSB

Enligt den nya dataskyddslagen och instruktion från Datainspektionen ska större personuppgiftsincident rapporteras till Datainspektionen inom 72 timmar. Dataskyddslagen kommer att träda i kraft som en svensk lag 1:a juni 2018 och behöver inte beslutas av Riksdagen

Samma sak kommer att gälla för alla incidenter som utgör ett hot mot deras nät och informationssystem och som på ett allvarligt sätt påverkar kontinuiteten för kritiska tjänster och tillhandahållandet av varor. Även om förslaget inte är förankrat som en svensk lag kommer troligen rapporteringsplikten att gälla rapportering till MSB, Myndigheter för samhällskydd och beredskap.

För att uppfylla detta krav behöver följande göras:

- Gör en felanmälan i Servicedesk och var tydlig med att ditt ärende rör en personuppgiftsincident för att it ska kunna klassificera ärendet korrekt.
- Fastställa riktlinjer för vad som klassas som personuppgiftsincident och vad som klassas som incident som utgör ett hot mot nät och informationssystem. För **personuppgiftsincident** finns redan en riktlinje från Datainspektionen som lyder enligt följande:
    1. enskilda förlorar kontrollen över sina uppgifter eller att deras rättigheter inskränks, vilket innebär
    2. att man utsätts för
        a. diskriminering,
        b. identitetsstöld,
        c. bedrägeri,
        d. finansiell förlust,
        e. skadlig ryktesspridning
        f. samt brott mot sekretess eller tystnadsplikt.

Ovanstående definition kan vara en bra beskrivning för personuppgiftsincidenter och läggas in i Servicedesk.

För bb hot mot nät och informationssystem gäller följande definition:

Störning som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten levererar till en annan organisation inom följande områden:

1. störning i mjuk- eller hårdvara,

2. störning i driftmiljö,

3. informationsförlust eller informationsläckage,

4. informationsförvanskning,

5. hindrad tillgång till information,

6. säkerhetsbrist i en produkt,

7. angrepp,

8. handhavandefel,

9. oönskad eller oplanerad störning i kritisk infrastruktur, eller

10. annan plötslig oförutsedd händelse som lett till skada.

Vem ska göra anmälan?

För en större personuppgiftsincident är det den personuppgiftsansvarige som ska göra anmälan, d v s ansvarig nämnd och det kan vi tolka som att det är den som är ansvarig för driften av registret som gör anmälan. För större hot mot nät och informationssystem gäller samma sak, d v s driftchef på it gör anmälan. Vid tveksamhet om anmälan ska göras rådgör driftchef med sektorchef eller kommunchef.

För en incident med flera källor/register finns inget uttalat om vem som ska göra anmälan, men samma rutin som ovan är en bra utgångspunkt, d v s anmäla görs av driftchef på it.

Vad ska anmälan innehålla?

Anmälan till Datainspektionen ska innehålla:

- Vilken typ av incident det är fråga om,
- Vilka kategorier av personer som kan komma att beröras,
- Hur många personer det berör,
- Vilka konsekvenser incidenten kan få samt
- Vilka åtgärder man vidtagit för att motverka ev. negativa konsekvenser

Anmälan till MSB ska innehålla:

- myndighetens namn,
- en beskrivning av it-incidenten som även inkluderar en övergripande
- redovisning av händelseförlopp och vidtagna åtgärder,
- den exakta eller uppskattade tidpunkten för när it-incidenten inträffade,
- när myndigheten upptäckte it-incidenten och om den alltjämt pågår eller
- är avslutad,
- till vilken eller vilka kategorier enligt 3 § som it-incidenten hör, samt
- myndighetens initiala bedömning av it-incidentens omfattning och
- konsekvenser, både faktiska och potentiella.

I rapporten ska om möjligt även anges bedömd sekretess för den information som rapporteras in.

För anmälan till MSB finns ett en särskild blankett

https://www.cert.se/it-incidentrapportering/Formular-for-it-incidentrapportering_MSB_F1v1_1.pdf