TRE SVENSKA LAGAR: NÄR GÄLLER VAD?

En jämförande analys av Dataskyddslagen (inkl GDPR), Cybersäkerhetslagen och Säkerhetsskyddslagen.

Introduktion:

Sverige har tre parallella lagstiftningar som reglerar cybersäkerhetsincidenter:

- **Datakyddslagen** kompletterar EU:s dataskyddsförordning GDPR och skyddar personuppgifter
- **Cybersäkerhetslagen** genomför NIS2-direktivet och träder i kraft den 15 januari 2026. Syftet är att uppnå en hög nivå av cybersäkerhet i samhället.
- **Säkerhetsskyddslagen** skyddar säkerhetskänslig verksamhet mot spionerі, sabotage och terrorbrott.

Analys:

De tre svenska cybersäkerhetslagarna har olika tillämpningsområden och syften som skapar en tydlig jurisdiktionshierarki. Säkerhetsskyddslagen har prioritet när verksamheten berör nationell säkerhet och stänger då av både Cybersäkerhetslagen (1 kap. 12 §) och GDPR:s rapporteringskrav Art. 33-34 (Dataskyddslagen 1 kap. 4 §), vilket innebär rapportering endast till Säkerhetspolisen. För verksamheter utan säkerhetskänslig anknytning kan Cybersäkerhetslagen och Dataskyddslagen gälla parallellt, vilket kräver rapportering till både sektorsspecifik tillsynsmyndighet t ex IVO för sjukvård och IMY vid personuppgiftsincidenter.

Lagarna kompletterar varandra genom att skydda olika intressen: Säkerhetsskyddslagen skyddar nationell säkerhet, Cybersäkerhetslagen skyddar samhällsviktig infrastruktur, och Dataskyddslagen skyddar individens personuppgiftsrättigheter.

Den största praktiska utmaningen uppstår för hybridorganisationer som bedriver både säkerhetskänslig och civil verksamhet. Dessa måste dela upp incidentrapportering per verksamhetstyp: säkerhetskänsliga delar rapporteras endast till SÄPO, medan civila delar omfattas av Cybersäkerhetslagen och eventuellt Dataskyddslagen med rapportering till respektive tillsynsmyndighet och IMY.

Myndigheternas ansvarsområden är tydligt uppdelade där IMY ansvarar för personuppgiftsskydd, sektorsspecifika tillsynsmyndigheter ansvarar för samhällsviktig cybersäkerhet, och Säkerhetspolisen ansvarar för nationell säkerhet.

Tillämpningsområde:

Lag	**Vem omfattas**	**Källor**
DSL (GDPR)	Alla som behandlar personuppgifter	DSL 1 kap 1 §
Cybersäkerhetslagen	Utvalda samhällskritiska sektorer, myndigheter med storlekskrav, undantag från storlekskrav finns.	Cybersäkerhetslagen 1 kap 1 §, 4 §

Säkerhetsskyddslagen	Verksamhet av betydelse för rikets säkerhet eller internationellt åtagande	Säkerhetsskyddslagen 1 kap 1 §

Vad rapporteras:

Lag	Incidenttyp	Definition
DSL (GDPR)	Personuppgiftsincident	“Säkerhetsintrång som leder till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt röjande av eller obehörig åtkomst till personuppgifter” - GDPR art 4 § 12
Cybersäkerhetslagen	Betydande cybersäkerhetsincident	Incident som påverkar tillhandahållande av tjänster eller verksamheter - Cybersäkerhetslag 4 kap 1 §
Säkerhetsskyddslagen	Säkerhetshotande IT-incident	IT-incident som "allvarligt kan påverka säkerheten" i informationssystem för säkerhetskänslig verksamhet - Säkerhetsskyddsförordning 2 kap 4 §

Rapporteringskrav:

Lag	Tidsgräns	Rapportera till
DSL (GDPR)	Inom 72 timmar från vetskap	IMY - GDPR art 33 § 1
Cybersäkerhetslagen	Inom 24 timmar (anmälan), inom 72 timmar (prel rapport), inom 30 dagar (slutrapport)	Tillsynsmyndighet - Cybersäkerhetslag 4 kap 6 §
Säkerhetsskyddslagen	Skyndsamt	Säpo, och Försvarsmakten om relevant - SSL 2 kap 1 §, SSF 2 kap 4 §

Flöde:

1. Är verksamheten säkerhetskänslig enligt Säkerhetsskyddslagen 1 kap. 1 §?
    a. JA - SÄKERHETSSKYDDSLAGEN HAR PRIORITET
        i. Ja, hela verksamheten:
            1. Rapportera till: SÄPO
            2. Cybersäkerhetslagen upphör helt enligt 1 kap 12 §
            3. Dataskyddslagen upphör enligt DSL 1 kap 4 § (refererar till GDPR Art 33-34)
        ii. Ja, delar av verksamheten:
            1. För säkerhetskänslig del:

            a. Rapportera till: SÄPO
            b. Cybersäkerhetslagen upphör helt enligt 1 kap 12 §
            c. Dataskyddslagen upphör enligt Dataskyddslagen 1 kap 4 § (refererar till GDPR Art 33-34)
        2. För icke-säkerhetskänslig del:
            a. Fortsätt till fråga 2
    b. NEJ - Fortsätt till fråga 2

2. Omfattas verksamheten av Cybersäkerhetslagen 1 kap. 4-5 §?
    a. JA - CYBERSÄKERHETSLAGEN GÄLLER
        i. Rapportera till: Tillsynsmyndighet
        ii. Fortsätt till fråga 3
    b. NEJ - Ingen rapportering inom ramen för Cybersäkerhetslagen
        i. Fortsätt till fråga 3

3. Innehåller incidenten personuppgifter enligt GDPR Art. 4(12)?
    a. JA - DATASKYDDSLAGEN GÄLLER
        i. Rapportera till: IMY inom 72 timmar från kännedom
    b. NEJ - Ingen rapportering inom ramen för Dataskyddslagen