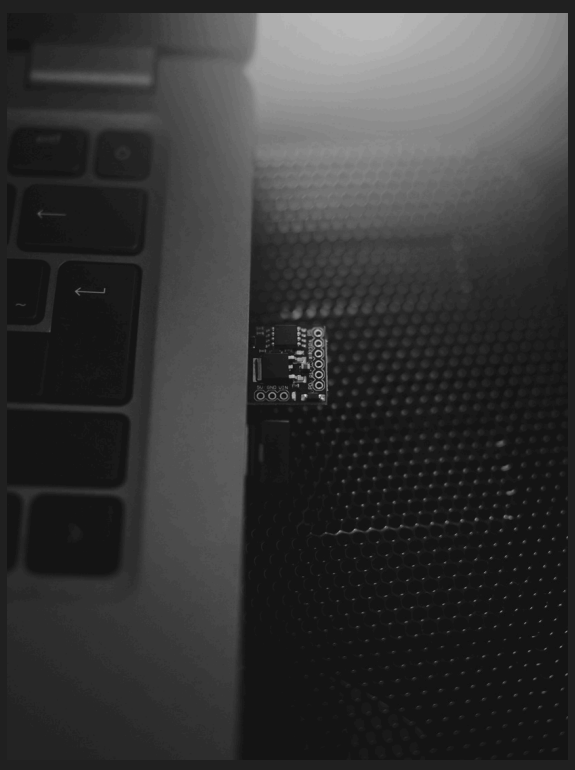
Cybersäkerhetslagen
(NIS2)

01
Vad handlar den nya cybersäkerhetslagen om?

Sverige och EU ska skyddas mot cyberhot! Cybersäkerhetslagen är en ny lag som kommer att börja gälla i Sverige i januari 2025. Digitaliseringen gör att cyberhot och cyberattacker ökar drastiskt, och nu kommer lagstiftning på området för att stärka Sverige och EU och vår gemensamma motståndskraft. Samtidigt ger de nya reglerna incitament för att företag ska jobba mer proaktivt med cybersäkerhet.

02
Varför är lagen så viktig?



Cybersäkerhetslagen är viktig eftersom den skyddar både individer och samhällen från hot i den digitala världen. I takt med att mer av vårt dagliga liv, affärer och statliga funktioner flyttar online, ökar också risken för cyberattacker som kan orsaka allvarliga skador. För företag kommer lagen vara en hygienfaktor i samarbeten och kundrelationer. Produkter, tjänster och till och med affärsmodeller kommer förväntas vara dokumenterat cybersäkra. Säkerhetsbrister kan leda till omfattande sanktionsavgifter, skadestånd i avtalsrelationer och förlorat förtroende från kunder som inte vill smittas av risk.

03
Vad måste företag göra?

I korthet så måste företag börja jobba mer proaktivt - och snabbare reaktivt, med cybersäkerhet:

1. **Avgör om du omfattas direkt eller indirekt av lagen – om du omfattas direkt - då måste du anmäla dig till aktuell tillsynsmyndighet.**
2. **Övervaka och analysera risker, skydda data.**
3. **Rapportera incidenter till tillsynsmyndigheter.**

Lagen ställer diverse krav på att företag och organisationer som driver viktiga samhällsfunktioner, som energi, transport och sjukvård, skyddar sig bättre mot cyberhot. Det handlar om att hela tiden ligga steget före i sitt skyddsarbete.

> För att korrekt uppfylla kraven krävs kompetens inom såväl IT-säkerhet och juridik. Morris Law har lång erfarenhet inom liknande complianceområden och kan skräddarsy den assistans du behöver tillsammans med andra experter.

04
Vilka är kraven?

De företag som omfattas av den nya cybersäkerhetslagen har en hel del administrativa krav som behöver uppfyllas. Några huvudsakliga uppgifter man måste vidta är följande:

- Identifiera att man omfattas och anmäla sig till relevant tillsynsmyndighet (varierar beroende på verksamhet)
- Etablera/upprätthålla ett systematiskt arbete med cybersäkerhet och införa lämpliga riskhanteringsåtgärder. Sådana ska vara baserade på en riskanalys och ett riskbaserat förhållningssätt.
- Utbildning för både ledning såväl som personal. Enligt den nya cybersäkerhetslagen så ska verksamhetens ledning genomgå utbildning och anställda ska erbjudas utbildning på det här området.
- Kravställ mot leverantörer. Den nya cybersäkerhetslagen har infört betydande förändringar för hur organisationer måste hantera sina leverantörer. Ett centralt krav är att företag måste utöva en så kallad due diligence på sina leverantörer, vilket innebär att man noggrant granskar deras säkerhetsåtgärder och förmåga att skydda känslig information. Detta ansvar omfattar hela leverantörskedjan och ställer högre krav på riskbedömningar och avtalsgranskning.
- Rapportera vissa cybersäkerhetsincidenter som medför eller kan medföra betydande störningar till tillsynsmyndighet. Det finns tidsramar att förhålla sig till. En varning ska in inom 24 timmar, incidentanmälan inom 72 timmar och en slutrapport inom en månad.
- Dokumentera! Ovanstående krav ska uppfyllas och dokumentation till stöd för detta ska kunna uppvisas vid en undersökning eller incident.

Vadå riskhanteringsåtgärder?

1. Incidenthantering
2. kontinuitetshantering,
3. säkerhet i leveranskedjan,
4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinfo,
5. strategier och förfaranden för användning av kryptografi och kryptering,
6. personalsäkerhet,
7. strategier för åtkomstkontroll och tillgångsförvaltning,
8. säkrade lösningar för kommunikation, och
9. lösningar för autentisering.

morris law.

05
Vad händer om man struntar i det? Eller bara misslyckas?

Företag som inte följer cybersäkerhetslagens krav riskerar att;

- **Drabbas av höga böter eller andra ekonomiska sanktioner. Sanktionsavgifterna kan utfärdas på upp till det högsta av 10 miljoner EUR eller 2% av global årsomsättning.**
- **Administrativa sanktioner ska även kunna riktas direkt mot företaget högsta styrande organ och personer i ledande ställning.**
- **Incidenter inom cybersäkerhet får ofta stora konsekvenser för många inblandade. Den som brustit riskerar omfattande krav på skadestånd från kunder och samarbetspartners.**
- **Företag som inte följer cybersäkerhetskrav riskerar att tappa kundernas och allmänhetens förtroende.**

06
Vilka branscher och företag berörs?

Cybersäkerhetslagen kommer att gälla alla stora och medelstora företag som deltar i leveransen av samhällskritiska tjänster, oavsett om de är offentliga eller privata. Från energibolag och banker till sjukhus och transportföretag. Även IT-företag såsom exempelvis leverantörer av molntjänster eller datacentraltjänster kan omfattas. I korthet anger lagen att alla företag som verkar inom 18 sektorer, ska omfattas av de nya kraven:

Sektorerna är följande:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Digitala leverantörer
- Forskning

I cybersäkerhetslagen kommer stora företag att definieras som verksamheter med fler än 250 anställda och en årlig omsättning om minst 50 miljoner euro. Medelstora företag definieras i sin tur som verksamheter med 50 till 249 anställda och en årlig omsättning om minst 10 miljoner euro.

Mindre företag och företag utanför sektorerna kan dock träffas indirekt såsom leverantörer till organisationer som träffas direkt av cybersäkerhetslagen.

Take aways i korthet

Cybersäkerhet är mer än teknik – det är en försäkring för framtiden!

Lagstiftningen på området är här och din organisation behöver sätta er in i de legala kraven som kommer och hur de kommer påverka ditt företags operativa arbete och framtid.

Se över rutiner och processer!

Ert företag behöver ha det nödvändiga systematiska arbetet internt för att kunna rapportera cybersäkerhetsincidenter till myndigheter snabbt och kontrollerat.

Arbeta hållbart med era leverantörer!

Företag kommer behöva ställa hårda krav på sina leverantörer för att upprätthålla cybersäkerhetslagens administrativa krav. Det är då viktigt att man jobbar hållbart och långsiktigt med leverantörer och uppställer rätt kravbild mot dem.

Påföljder om du missar!

Ignorerar man lagen riskerar man både böter och ett dåligt rykte. Säkerhet är inget man kan snåla på längre!

Kontakta oss om du vill ha hjälp eller få mer info

Henrik Almström
Specialist Counsel, Advokat
henrik.almstrom@morrislaw.se
+46 738 26 47 75

Karin Odkrans
Senior Associate, Advokat
karin.odkrans@morrislaw.se
+46 708 83 73 46

Mathilda Kronér
Associate
mathilda.kroner@morrislaw.se
+46 708 44 02 44

morris law.