Cybersecurity: de Cyberbeveiligingswet (NIS 2)

De samenleving is sterk afhankelijk geworden van digitale technologieën. Deze technologieën brengen een enorme efficiëntieslag met zich mee op vele gebieden. Maar er zijn ook risico's. Veel bedrijven kunnen door deze afhankelijkheid van technologie volledig stil komen te liggen systemen niet meer werken.

Sommige organisaties mogen niet stil komen te liggen, vanwege de maatschappelijke gevolgen die dat zou hebben. Denk bijvoorbeeld aan gezondheidszorg, overheid of de levensmiddelensector. De Cyberbeveiligingswet, de implementatiewet van de NIS-2 richtlijn, beoogt dit te voorkomen door nieuwe cybersecurity verplichtingen op te leggen. De wet treedt naar verwachting in 2026 in werking.

Wat regelt de Cyberbeveiligingswet?

De Cyberbeveiligingswet heeft als doel het niveau van cybersecurity omhoog te krijgen. Daarvoor roept het een aantal verplichtingen en nieuwe regels in het leven:

- **Beveiligingsmaatregelen,** zoals het toepassen van encryptie.
- **Meldplicht** bij incidenten die kunnen leiden tot een verstoring van essentiële diensten.
- **Extra handhavingsbevoegdheden** voor toezichthoudende autoriteiten.
- **Hogere sancties.** Er kunnen boetes opgelegd worden tot 10 miljoen euro.
- **Boetes voor bestuurders** als het beveiligingsbeleid niet op orde is.

Ook leveranciers van organisaties die onder de Cyberbeveiligingswet vallen moeten aan deze wet voldoen. Daarmee is de Cyberbeveiligingswet ook erg relevant voor bijvoorbeeld **IT-leveranciers.** Lees hier meer over de nieuwe regels uit de Cyberbeveiligingswet en de Richtlijn.

Roadmap naar compliance

De verplichtingen uit de Cyberbeveiligingswet kunnen invloed hebben op uw gehele bedrijfsvoering. Het is belangrijk dat u op tijd begint met het controleren of u al aan deze voldoet. Onze specialisten kunnen u adviseren, bijvoorbeeld over:

- Is de Cyberbeveiligingswet van toepassing op mijn organisatie?
- Welke maatregelen moet ik treffen?
- Voldoen mijn overeenkomsten aan de vereisten van de Cyberbeveiligingswet?
- Hebben mijn bestuurders voldoende kennis over cybersecurity en het interne cybersecurity-beleid?

Heeft u vragen? Neem contact op met Ruben Krul, Pieter Ballings, Kim de Bonth of Femmie Schets.

Gijs van Berkel
+31 (0) 88 44 02 321
g.vanberkel@holla.nl

Pieter Ballings
+31 88 44 02 340
p.ballings@holla.nl

Kim de Bonth
+31 (0) 88 44 02 374
k.debonth@holla.nl

Femmie Schets
+31 (0) 88 44 02 333
f.schets@holla.nl