BOLT THE DATA LAWYERS

BASIS CHECKLIST CYBERSECURITY REGELS

Door nieuwe (Europese) cybersecurity regelgeving moeten steeds meer organisaties voldoen aan cybersecurityregels. Dit om de digitale weerbaarheid van organisaties te vergroten. Twee belangrijke regelingen zijn de NIS2 (Network and Information Security (NIS2) directive) en de DORA (Digital Operation Resilience Act).

De regelgeving is van toepassing op bedrijven en organisaties in bepaalde sectoren en op kritieke ICT toeleveranciers van de bedrijven en organisaties in die sectoren. Ook worden leidinggevenden verantwoordelijk en aansprakelijk voor het managen van cyber risico's en moeten zij trainingen volgen.

Met deze checklists kunnen bedrijven en andere organisaties nagaan of de nieuwe wet- en regelgeving van toepassing is, aan welke verplichtingen zij moeten voldoen en welke stappen zij in ieder geval moeten nemen. De checklists bevatten concrete acties waar uw bedrijf of organisatie direct mee aan de slag kan gaan.

Stap 1: Is de NIS2 of DORA van toepassing op mijn organisatie?

- ☐ Stel vast of uw organisatie onder de NIS2 of DORA valt. Zie Checklist NIS2 / DORA van toepassing?

↓

Stap 2: Welke beleidsstukken moet mijn organisatie opstellen of aanpassen

- ☐ Stel vast of uw organisatie alle verplichte beleidsstukken heeft geïmplementeerd in lijn met NIS2 en / of DORA. Zie de Checklist Cybersecurity Beleidsstukken voor informatie over:
  - ☐ Incident response
  - ☐ Algemeen beleid
  - ☐ Meldplichten

↓

Stap 3: Zijn de contracten van mijn organisatie up-to-date?

- ☐ Stel vast of de contracten van uw organisatie up-to-date zijn. Zie Checklist Up-to-date Contracten voor meer informatie over:
  - ☐ Inventarisatie IT contracten
  - ☐ Overzicht relevante artikelen per contract

Stap 4: Welke verzekeringen moet mijn organisatie afsluiten?

- ☐ Stel vast of uw organisatie de volgende verzekeringen dient af te sluiten:
  - ☐ Beroepsaansprakelijkheidsverzekering
  - ☐ Bedrijfsaansprakelijkheidsverzekering
  - ☐ Cybersecurityverzekering
  - ☐ Bestuurdersaansprakelijkheidsverzekering
- ☐ Zie de Checklist Aandachtspunten afsluiten verzekeringen voor meer informatie over:
  - ☐ Bestuurdersaansprakelijkheid onder de NIS2/DORA
  - ☐ Checklist cybersecurity- en beroepsaansprakelijksverzekeringen

Stap 5: Hoe informeer en train ik het personeel en de leidinggevenden/ bestuurders?

- ☐ Stel de leidinggevenden/ bestuurders en werknemers op de hoogte van basispraktijken op het gebied van cyberbeveiliging. Zie de Checklist Cybersecurity Beleidsstukken onder 'training'.

OVERZICHT CYBERSECURITY CHECKISTS

- ✓ Checklist NIS2/DORA van toepassing: met uitleg over classificatie als 'belangrijke' of 'essentiële' entiteit.
- ✓ Checklist Cybersecurity beleidsstukken: met een uitgebreid overzicht van alle verplichte beleidstukken, incident response en meldverplichtingen.
- ✓ Checklist Up-to-date contracten: met een uitgebreid overzicht van relevante contractsbepalingen zoals beveiliging en aansprakelijkheid.
- ✓ Checklist Aandachtspunten verzekeringen: met een overzicht van de belangrijkste aandachtspunten in het kader van verschillende type verzekeringen.

Training bestuurders

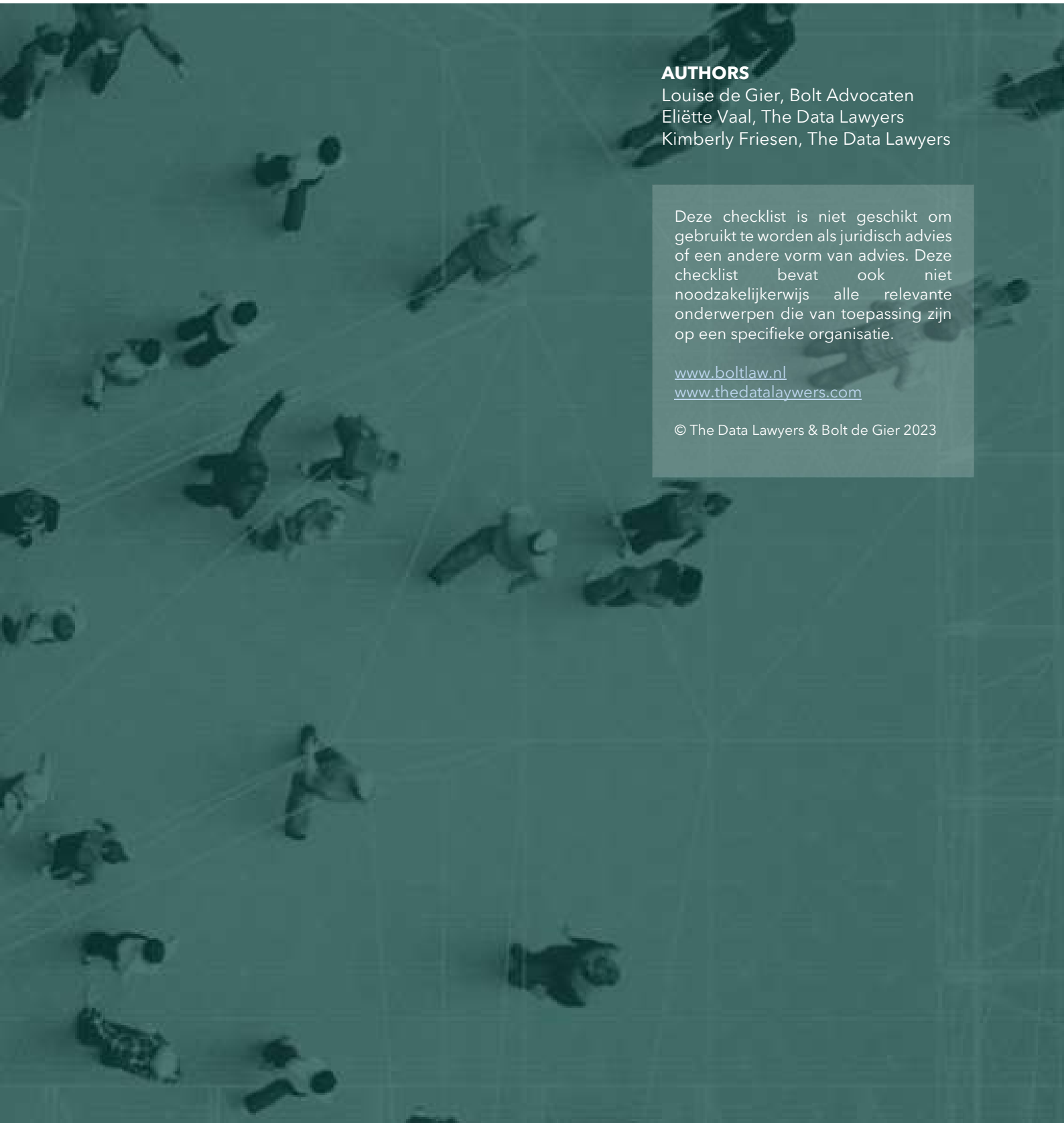
Bestuurders kunnen aansprakelijk worden gesteld voor het niet naleven van de cybersecurity regels. Daarnaast bevatten zowel NIS2 als de DORA verplichtingen voor het bestuur om cybersecurity trainingen te volgen. Een concrete actie voor uw bedrijf of organisatie is het opzetten van trainingen voor werknemers, maar ook voor het bestuur.

Nieuwe meldplichten

In de NIS2 en DORA zijn specifieke meldplichten vastgelegd waar bedrijven en organisaties aan moeten voldoen nadat er (mogelijk) een IT-beveiligingsincident heeft plaatsgevonden. De NIS2 en DORA bevatten gedetailleerde regels over wie, wanneer, op welke manier moet worden geïnformeerd. Het is belangrijk dat uw bedrijf en/ of organisatie goed voorbereid is op mogelijke IT-beveiligingsincidenten, zodat uw bedrijf of organisatie adequaat kan reageren in een crisissituatie.

HULP BIJ IMPLEMENTATIE

De checklists vormen het startpunt voor het implementeren van beleid, beoordelen van aansprakelijkheid, updaten van contractuele verplichtingen en implementeren van een compliant incident response plan. Op basis van de checklists beoordelen wij graag met uw bedrijf of organisatie het effect van cybersecurityregelgeving. Neem contact op voor meer informatie.



AUTHORS
Louise de Gier, Bolt Advocaten
Eliëtte Vaal, The Data Lawyers
Kimberly Friesen, The Data Lawyers

Deze checklist is niet geschikt om gebruikt te worden als juridisch advies of een andere vorm van advies. Deze checklist bevat ook niet noodzakelijkerwijs alle relevante onderwerpen die van toepassing zijn op een specifieke organisatie.

www.boltlaw.nl
www.thedatalaywers.com