Integraal Risicomanagement
NIS2-Richtlijn
AI Verordening

Hoogheemraadschap van
Rijnland

Inhoudsopgave

- Waar staan we?
- Waar willen we naar toe?
- Overzicht wetgeving
- Richtlijn / Verordening
- NIS2-richtlijn
- AI Verordening
- Checklist: *eerste aanzet*

Waar staan we nu?

- Alle systemen hebben een eigenaar.
- De ‘kroonjuwelen’ zijn geïdentificeerd en maatregelen bekend.
- Beleid voor integraal samenwerken aan beveiliging.
- Solide techniek met veel mogelijkheden voor beveiliging.
- Monitoring kantoor- en procesautomatisering in werking.
- Calamiteitenplan gereed en de oefening gepland.
- Awareness sessies op alle lagen van de organisatie.

Waar willen we naar toe?

- Alle systemen op vastgesteld beveiligingsniveau.
- De ‘kroonjuwelen’ behalen volwassenheidsniveau 4.
- Risico’s worden integraal bepaald en gemitigeerd.
- Uitnutten E5 licentie voor beveiliging.
- Optimalisatie monitoring.
- Calamiteitenplan met PDCA.
- Medewerkers zijn risicobewust en digitaal vaardig.

Richtijn & Verordening

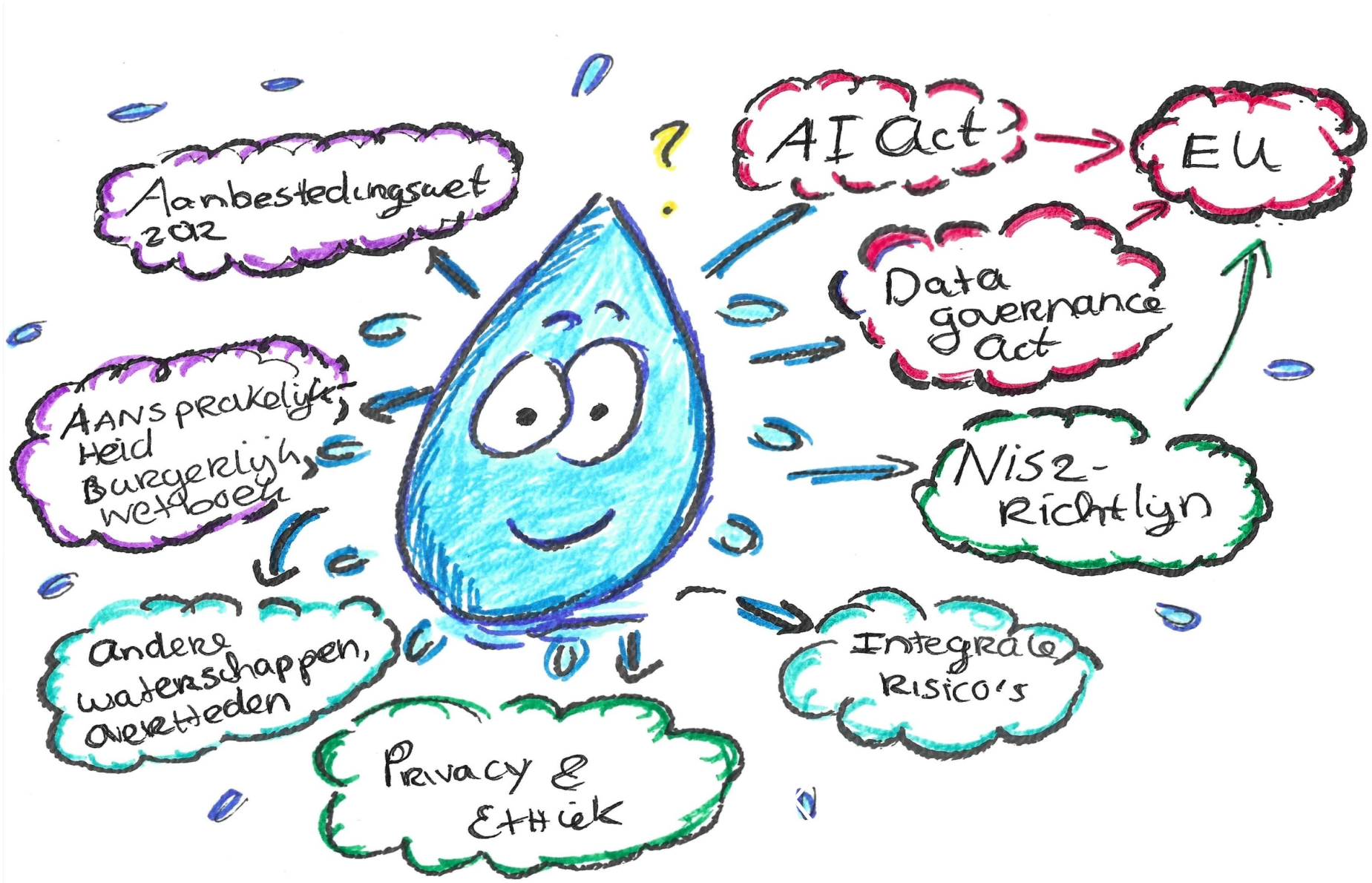
- **Verordening**: Direct bindend, rechtstreeks van toepassing en uniform voor alle EU-lidstaten.

- **Richtlijn**: Stelt een algemeen doel vast. De EU-lidstaten moeten voor 17 oktober 2024 zelf de richtlijn omzetten in nationale wetgeving.

  De Minister heeft laten weten dat het Nederland niet gaat lukken om de NIS2-richtlijn (en de CER-richtlijn) tijdig te implementeren.

  Bepalingen die ‘onvoorwaardelijk en voldoende nauwkeurig zijn’ hebben rechtstreekse werking. Een te late implementatie kan leiden tot boetes en tot aansprakelijkheid.

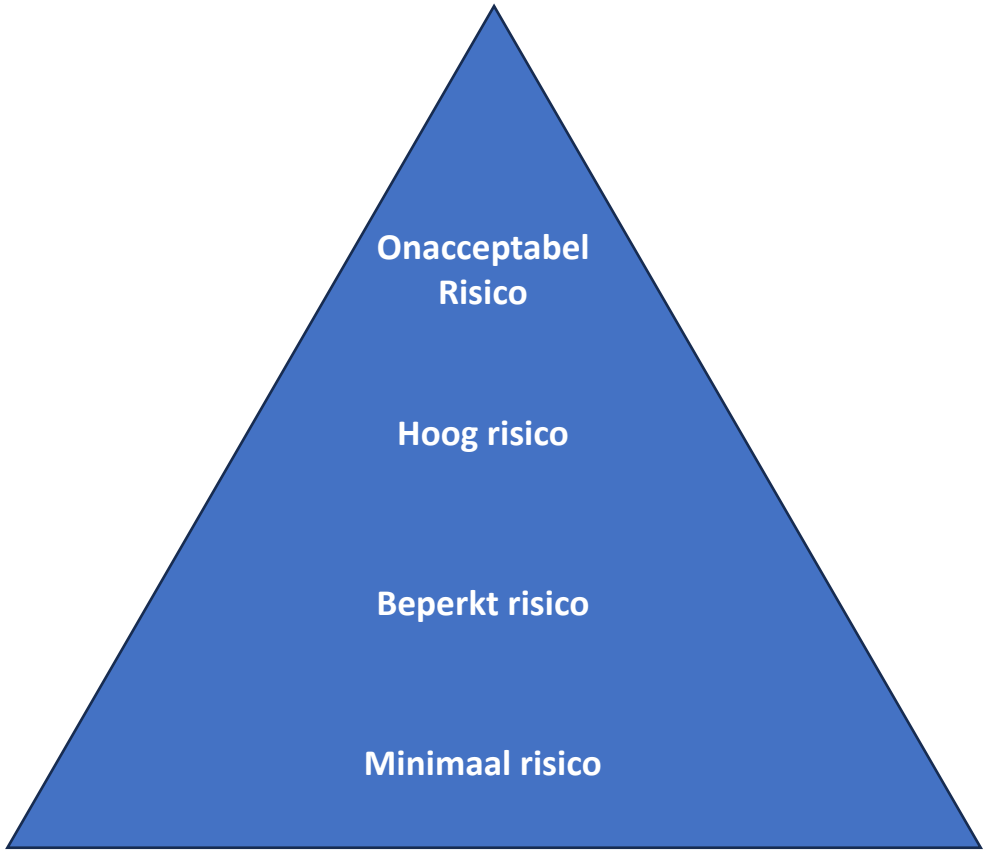
Overzicht wetgeving



NIS2-richtlijn

NIS2-richtlijn	Uitleg
Toepassingsgebied	De NIS2-richtlijn is van toepassing op sectoren zoals energie, transport, bankwezen, gezondheid, digitale infrastructuur en meer. Organisaties met minimaal 50 werknemers of een jaaromzet van minimaal €10 miljoen vallen binnen het toepassingsgebied. Entiteiten die vallen onder de NIS2-richtlijn zijn verplicht zich te registreren.
Risicobeheer en rapportage	Rijnland moet risicobeoordelingen uitvoeren, risico's in kaart brengen en cyberbeveiligingsmaatregelen nemen. Dit geldt ook voor de toeleverancierskеten. Rapportages moeten inzicht bieden in de strategie, risico's en de te nemen beheersmaatregelen.
Meldingsplicht	Bij incidenten moet Rijnland tijdig voldoen aan de meldingsverplichtingen.
Boete(s) voor essentiële entiteiten	Niet-naleving van de NIS2-richtlijn kan leiden tot boetes tot €10 miljoen of 2% van de wereldwijde jaaromzet.
Bestuurdersaansprakelijkheid	In art. 32 lid 6 van de NIS2-richtlijn staat dat iedere bestuurder wettelijk bevoegd dient te zijn om security-maatregelen te nemen. Een bestuurder kan aansprakelijk worden gesteld wanneer zij de NIS2-richtlijn niet naleven. Daarnaast geldt ook het nationale aansprakelijkheidsrecht.
Zorgplicht	Rijnland moet kunnen aantonen dat de netwerk- en informatiesystemen voldoen aan risicomaatregelen.
Toezicht	Rijnland moet rekening en verantwoording afleggen en aantoonbaar voldoen aan de eisen uit de Richtlijn. De toezichthouder zal dit controleren.
Risicobewustzijn	Rijnland moet cyber- en netwerkrisico's proactief identificeren en acteren door het nemen van beheersmaatregelen.

AI Verordening (1)

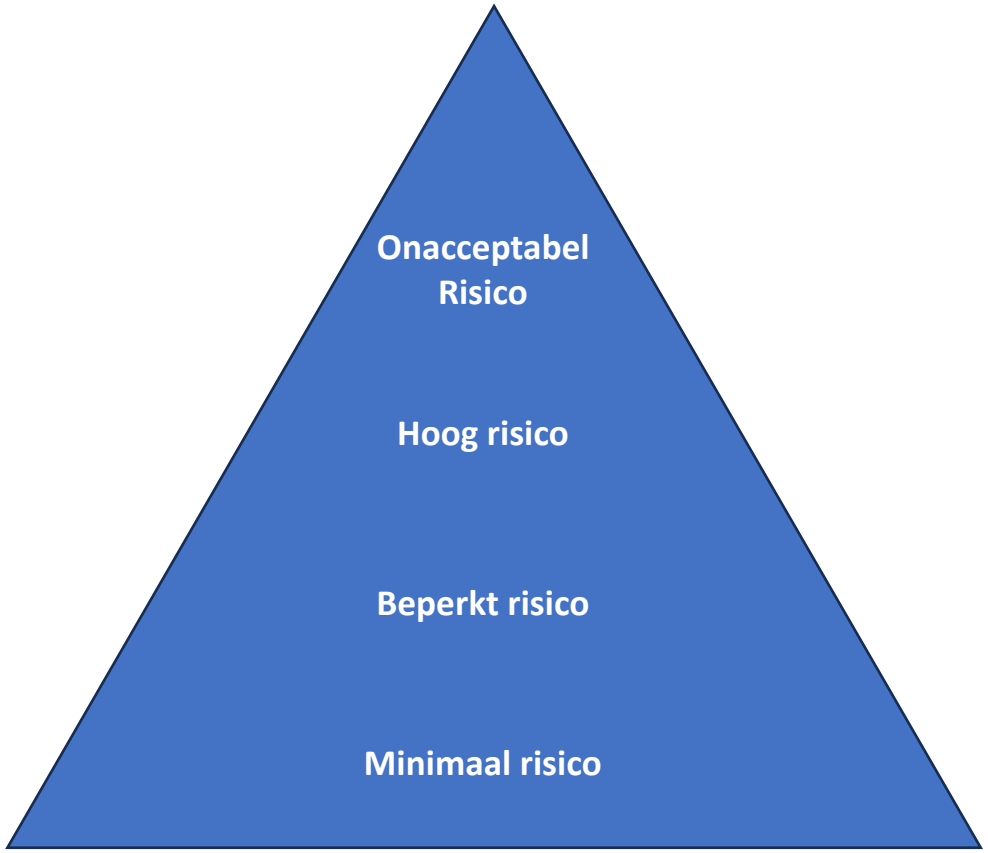


- Het gaat om AI systemen die vallen binnen de reikwijdte van de verordening. Wij stellen het risico niveau vast en op basis daarvan schrijft de verordening voor wat de verplichtingen zijn.

- AI systemen met een onacceptabel risico voor burgers zijn verboden. Denk bijv. aan: biometrische Identificatiesystemen en social scoring.

- Hoe hoger het risico van een AI-systeem, hoe hoger de transparantie moet zijn qua werking, informatie en besluitvorming. Wij moeten in staat zijn om uit te leggen hoe een systeem tot bepaalde resultaten komt.

AI Verordening (2)



- AI Verordening zal zorgen voor nieuwe compliance en beveiligingsverplichtingen.
- Bij AI systemen met risicovolle toepassing, is menselijke tussenkomst vereist.
  Er mag geen black box zijn.
- Bewijslast zal verschuiven. Aanname van causaal verband bij een fout.
- Aansprakelijkheid geldt ook in de toeleverancierskketen.

AI Verordening

AI Verordening (AI ACT)	Uitleg
Doel	Innovatie stimuleren, de veiligheid en naleving van grondrechten waarborgen en onze democratische rechtstaat beschermen.
Toepassing	Op 13 maart 2024 heeft het Europese Parlement de AI Verordening aangenomen.
Basismodellen (zoals Bing Chat en ChatGPT)	Ontwikkelaars van basismodellen moeten al na 12 maanden na inwerkingtreding AI verordening, dus begin 2025, voldoen aan de wet.
Gereguleerde AI systemen	AI systemen van gereguleerde producten moeten binnen 36 maanden na inwerkingtreding AI Verordening voldoen aan de wet.
Verboden systemen	Al 6 maanden, na inwerkingtreding van de AI Verordening, moet iedere lidstaat hard optreden tegen verboden systemen.
Transparantieverplichting	Wij moeten actief toezicht houden op de naleving van de transparantieverplichtingen in de toeleverancierssketen. Gebruikers moeten goed geïnformeerd zijn over de voorwaarden.
Risicobeoordeling	Rijnland moet een risicobeoordeling uitvoeren voor AI-systemen die we inzetten.
Boete	Een boete bedraagt maximaal 35 miljoen euro of 7 procent van de wereldwijde omzet, afhankelijk van de overtreding en de grootte van het bedrijf.

Checklist: *eerste aanzet (1)*

- **Risicobeoordeling**
  - Is er een integrale risicobeoordeling uitgevoerd?
  - Wie houdt er toezicht en is belast met audits?
- **Beveiligingsmaatregelen**
  - Zijn er specifieke beveiligingsmaatregelen geïmplementeerd om Rijnland te beschermen tegen cyberaanvallen?
- **Transparantie en Uitlegbaarheid**
  - Is de technische oplossing begrijpelijk en uitlegbaar?
  - Welke data gebruiken wij?
  - Past de technische oplossing binnen de bestaande processen?

Checklist: *eerste aanzet (2)*

- **Verantwoordelijkheid**
  - Wie is juridisch verantwoordelijk voor de technische (AI-)oplossing?
  - Wie is waarvoor aansprakelijk in de keten?
- **Identificatie en Classificatie**
  - In welke risico-categorie valt deze technische oplossing op basis van AI Verordening?
  - Kunnen wij de resultaten begrijpen en controleren?
- **Opleiding en bewustwording**
  - Zijn medewerkers op de hoogte van de risico's en voldoende opgeleid?
- **Privacy en Ethiek**
  - Voldoen wij aan de privacy wet- en regelgeving?
  - Op welke manier is rekening gehouden met de ethische aspecten en menselijke tussenkomst?

Vragen?