Regelgeving

Cyberboswachters

Tim Dams

Deze cursus werd gemaakt met hulp van AI-assistentie. Sommige afbeeldingen zijn door AI gegenereerd.

Cyberboswachters
AI GENERATED

Wat leer je in dit deel?

Na dit deel kan je:

- ✓ de **rechten** die de **GDPR** je geeft en de plichten van bedrijven bij een datalek uitleggen
- ✓ inschatten of een organisatie onder de **Belgische NIS2-wet** valt, en of ze **essentieel** of **belangrijk** is
- ✓ de rol van het **CCB**, de **aansprakelijkheid van bestuurders** en **CyberFundamentals** toelichten
- ✓ de verplichtingen van de **Cyber Resilience Act** voor fabrikanten opsommen
- ✓ de **meldplichten** van GDPR, NIS2 en CRA naast elkaar zetten

Waarom moet een informaticus dit kennen?

GDPR

Je app bewaart namen of e-mailadressen? Dan moet jij zorgen dat een datalek geen ramp wordt.

NIS2

Je werkgever is een ziekenhuis, waterbedrijf of IT-dienstverlener? Een ernstig incident meld je binnen **24 uur**.

CRA

Je bouwt een product met software erin? Dan moet het veilig op de markt komen en jarenlang updates krijgen.

VERORDENING OF RICHTLIJN?

Een **verordening** (GDPR, CRA) geldt meteen en overal in de EU, woord voor woord.

Een **richtlijn** (NIS2) legt enkel de doelen vast: elke lidstaat zet ze om in een eigen wet. Vandaar “de **Belgische** NIS2-wet”.

ETHISCH HACKEN EN DE WET

Sinds **februari 2023** is ethisch hacken legaal in België, mits je het lek meldt bij het bedrijf **én** het CCB.

Die regels staan intussen in de **NIS2-wet** (artikels 22 en 23).

DEEL 1

GDPR

De strengste privacywet ter wereld, sinds **25 mei 2018**.

> The toughest privacy and security law in the world.

— gdpr.eu, over GDPR

2018

Wat is GDPR?

General Data Protection Regulation, in het Nederlands de *Algemene Verordening Gegevensbescherming*.

Personen in de EU

Beschermt de privacy van wie zich **in de EU** bevindt. Je nationaliteit speelt geen rol.

Iedere organisatie

Wie een vestiging in de EU heeft of data van mensen in de EU verwerkt, valt eronder. Ook buiten Europa, ook overheden en vzw's.

99 artikels

Over de rechten van burgers en de plichten van bedrijven.

GDPR gaat over de plichten van **bedrijven**, niet van personen.

De wet beschermt de burger tegen de bedrijven die zijn data verzamelen, en weet haar regels ook **buiten Europa** af te dwingen.

Jouw rechten

Vergeten worden	Data over jou laten wissen (met uitzonderingen)
Inzage	Weten welke data een bedrijf over jou heeft
Rectificatie	Foute data laten corrigeren
Beperking	Verwerking (tijdelijk) laten stoppen
Verzet	Je verzetten tegen het gebruik van je data
Geautomatiseerde besluitvorming	Geen belangrijke beslissing die enkel door een computer genomen wordt
Portabiliteit	Je data in een gestructureerde, machineleesbare vorm, door te sturen naar een ander bedrijf
Minimalisatie en opslagbeperking	Bedrijven verzamelen enkel wat ze nodig hebben, en bewaren het niet langer dan nodig

RECHT OM VERGETEN TE WORDEN

Je kan een bedrijf verplichten om **alle of specifieke data** over jou te wissen. Niet absoluut: een wettelijke bewaarplicht of de vrijheid van meningsuiting kan voorgaan.

Ook zoekmachines: moet Google je huisadres niet kennen, dan kan je Google verplichten die info te verwijderen.

In 2020 kreeg **Google Belgium** van de GBA een boete van **€ 600.000** omdat het niet inging op zo’n vraag van een Belgische burger.

Recht op overdraagbaarheid

⚠ Vroeger

- Elk bedrijf had zijn **eigen dataformaten**
- Bij een overstap moest alles omgezet worden
- Van provider veranderen was een helse opdracht

vs

Met GDPR

- Je data in een **gestructureerd, machineleesbaar** formaat
- Waar mogelijk rechtstreeks doorgestuurd naar het nieuwe bedrijf
- Overstappen zonder administratieve rompslomp

De voorganger van GDPR, de **DPD** (1995), was een richtlijn: elk land maakte er zijn eigen versie van.

Welke data beschermt GDPR?

Identiteit

Naam, adres, geboortedatum, rijksregisternummer

Wat je online doet

Locatie, IP-adres, cookies

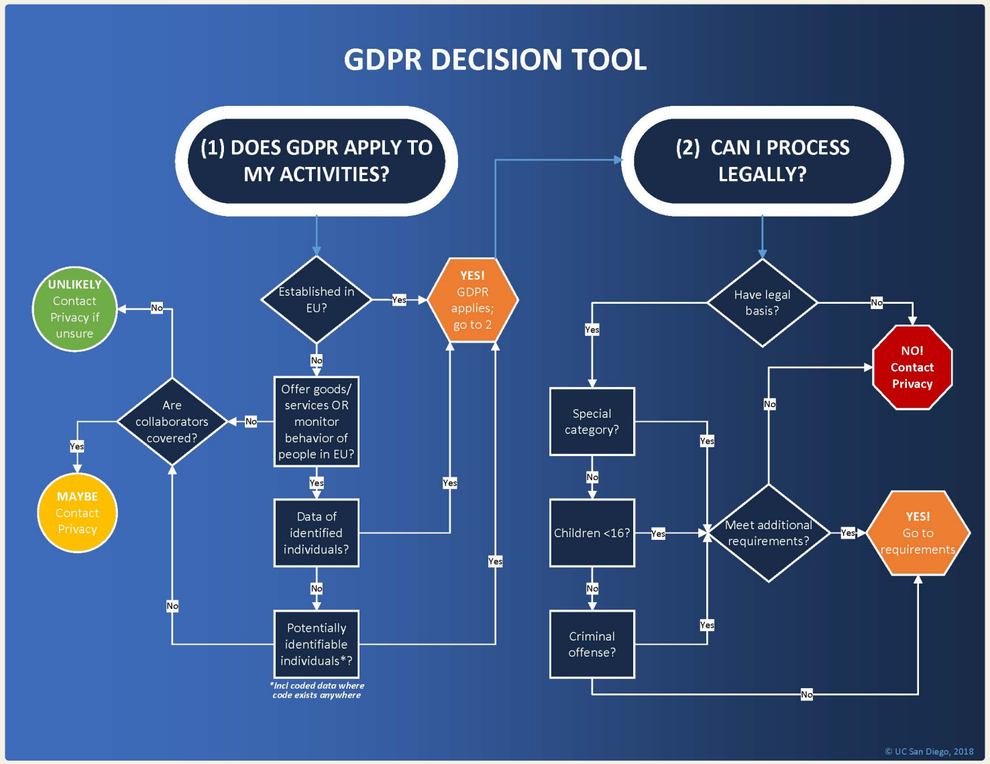
Je lichaam

Gezondheids- en genetische gegevens, biometrie (irisscan, vingerafdruk)

Heel persoonlijk

Raciale of etnische gegevens, politieke meningen, seksuele geaardheid

GDPR in twee vragen



Geldt de GDPR, en mag ik verwerken? “Contact Privacy” = je privacyverantwoordelijke of DPO (Bron: privacy.ucsd.edu/gdpr/).

Kinderen: de GDPR legt de grens op **16 jaar**, België verlaagde die naar **13**.

Persoonlijke data buiten de EU

Binnen de EU (en EER) reist data vrij. Daarbuiten moet de **bescherming mee reizen**. Ook toegang vanop afstand telt als doorgifte.

Adequaatheidsbesluit

De Commissie keurt het land goed: Zwitserland, VK, Japan, Canada, Brazilië, …

Standaardcontract

SCC's tussen verzender en ontvanger, plus nagaan of de wetten daar ze niet onderuit halen

Uitzondering

Occasioneel: uitdrukkelijke toestemming of nodig voor een contract (hotel in Thailand)

EU - VS

Het pingpongspel

1. **2000**: Safe Harbor
2. **2015**: ongeldig verklaard door het Hof (*Schrems I*)
3. **2016**: Privacy Shield
4. **2020**: ook ongeldig (*Schrems II*)
5. **2023**: EU-US **Data Privacy Framework**, beroep bij het Hof loopt nog

Meta kreeg in 2023 **€ 1,2 miljard** boete: na *Schrems II* bleef het Facebook-data naar de VS sturen.

> Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot persoonsgegevens.

— Definitie van een datalek

MELDPLICHT

72 uur

om een datalek te melden aan de toezichthouder, te rekenen vanaf de **ontdekking** van het lek

Het lek zelf kan dus al maanden eerder gebeurd zijn: de klok start pas als het bedrijf het ontdekt. Nog niet alle info? Dan mag je de melding in stappen aanvullen.

Geen waarschijnlijk risico voor de betrokkenen? Dan hoef je niet te melden, maar wel **intern documenteren**.

Melden aan wie?

De toezichthouder

In België de **GBA** (*Gegevensbeschermingsautoriteit*), vroeger de privacycommissie. Zo mogelijk binnen **72 uur**.

De betrokkenen

Bij een **hoog risico** ook iedereen wiens data gelekt is, zonder onredelijke vertraging.

Of: publiek

Moeten er erg veel mensen verwittigd worden, dan mag ook een **publieke aankondiging**. Altijd een PR-nachtmerrie.

Wanneer hoeft het individu het niet te weten?

Data is onbruikbaar

De gestolen data was **geëncrypteerd**: de aanvallers kunnen er niets mee.

Kanttekening: encryptie is nooit 100% waterdicht. Decryptie in de toekomst blijft mogelijk.

Data is niet herleidbaar

Voorkeuren en identificeerbare gegevens staan in **aparte databases**.

Enkel de voorkeuren gelekt? Dan is er geen privacyschending.

Don't put all your eggs in one basket: bewaar data verspreid over **meerdere databases**.

Hoe hoog kan een boete zijn?

2%

van de wereldwijde jaaromzet of **€ 10 miljoen** bij minder ernstige inbreuken

4%

van de wereldwijde jaaromzet of **€ 20 miljoen** bij inbreuken op de kern van GDPR: het recht op privacy en het recht om vergeten te worden

Telkens het **hoogste** bedrag van de twee.

BOETE OF NIET? DAT HANGT AF VAN

- Ernst en aard
- Intentie: slordigheid of opzet?
- Schadebeperking
- Genomen voorzorgen
- Geschiedenis van overtredingen
- Medewerking met de autoriteiten
- Gegevenscategorie
- Meldplicht nageleefd?
- Certificering (externe audit)
- Verzwarende of verzachtende factoren

Een schending leidt dus **niet automatisch** tot een boete.

GDPR in de praktijk

€ 7,1 miljard

aan boetes in Europa tussen mei 2018 en begin 2026

€ 1,2 miljard

voor **Meta** (2023): het record

€ 530 miljoen

voor **TikTok** (2025): data van Europeanen onvoldoende beschermd tegen inzage vanuit China

Gemiddeld worden er in Europa **443 datalekken per dag** gemeld.

FAQ

Mag dat?

Camera die de straat filmt

Nee. Enkel je eigen eigendom. Buitencamera: aangifte via aangiftecamera.be, pictogram, beelden max. **1 maand** bewaren.

Winkel die je eID inleest

Enkel met je **toestemming** of als een wet het verplicht. Weigeren mag. Alcohol? Enkel je geboortedatum.

Foto van iemand online

Toestemming om te fotograferen is **niet** hetzelfde als toestemming om te publiceren. Kinderen: beide ouders.

FAQ

Je rechten in de praktijk

Cookies

Enkel strikt noodzakelijke cookies zonder toestemming. Geen vooraf aangevinkte vakjes, geen cookiemuur.

Inzageverzoek

Gratis, antwoord binnen **1 maand**. Geen reactie? Bemiddeling of klacht bij de GBA. Misbruik om geld te innen mag geweigerd worden.

Schadevergoeding

Kan, ook voor **angst** na een lek. Wel schade aantonen. De Commissie betaalde zelf **€ 400** voor “Inloggen met Facebook”.

FAQ

Voor de informaticus

Meneer of mevrouw?

Het Hof (2025): een treinticket verkopen kan **zonder** geslacht. Elk verplicht veld: waarvoor heb ik dit nodig?

Gehasht = anoniem?

Nee. Wie kan terugkoppelen, verwerkt nog persoonsgegevens. Enkel echte anonimisering valt buiten de GDPR.

Echte klantendata als testdata?

Liefst niet: ook dat is een verwerking, en testomgevingen zijn vaak slecht beveiligd. Gebruik fictieve data.

Mails lezen als sysadmin?

Technisch kunnen is niet mogen. Enkel binnen de ICT-policy (**cao 81**): doel, proportioneel, transparant.

Is de GDPR veranderd?

1

2018: de tekst van de GDPR is sindsdien niet gewijzigd

→

2

2 april 2027: procedureverordening, vaste termijnen voor klachten tegen bedrijven in meerdere landen (max. 15 maanden)

→

3

Digital Omnibus: o.a. meldplicht naar 96 uur, nieuwe definitie persoonsgegevens. Nog in onderhandeling, **geen wet**

DEEL 2

NIS2

Welke organisaties moeten zich beveiligen, en wat als het misloopt?

13 JANUARI 2026, 6U32

Een cyberaanval (volgens de pers ransomware) verstoort het Antwerpse ziekenhuis AZ Monica. Uit voorzorg gaan alle servers plat.

Operaties geschrapt, spoed op halve kracht, zeven kritieke patiënten overgebracht. En ondertussen tikt er een wettelijke klok: het CCB moet binnen **24 uur** verwittigd worden.

Van richtlijn naar Belgische wet

1. **14 december 2022**: Europese NIS2-richtlijn (EU 2022/2555)

→

2. **26 april 2024**: Belgische NIS2-wet, gepubliceerd op 17 mei 2024

→

3. **18 oktober 2024**: in werking, zorgplicht en meldplicht gelden

→

4. **18 maart 2025**: registratie bij het CCB via Safeonweb@Work

Wie valt eronder?

Sector

- **Bijlage I** (hoge kriticiteit): energie, vervoer, banken, gezondheidszorg, drinkwater, digitale infrastructuur, ICT-dienstverleners, overheid, …
- **Bijlage II** (andere kritieke): post, afval, chemie, levensmiddelen, maakindustrie, digitale aanbieders, onderzoek

vs

Grootte

- **Middelgroot**: vanaf 50 werknemers, of meer dan 10 miljoen euro omzet **én** balanstotaal
- **Groot**: vanaf 250 werknemers, of meer dan 50 miljoen euro omzet **én** 43 miljoen balanstotaal
- Kleiner? Dan meestal niet, op enkele uitzonderingen na (bv. DNS, `.be`-register)

Essentieel of belangrijk?

	Essentiële entiteit	Belangrijke entiteit
Wie?	Vooral **grote** organisaties uit bijlage I	Middelgrote uit bijlage I, alle middelgrote en grote uit bijlage II
Toezicht	**Proactief**: verplichte conformiteitsbeoordeling	**Reactief**: na aanwijzingen of een incident
Maximale boete	€ 10 miljoen of 2%	€ 7 miljoen of 1,4%

De verplichtingen zijn dezelfde. Het verschil zit in hoe streng er gecontroleerd wordt.

Vlaamse voorbeelden

Essentieel

Een groot ziekenhuis zoals AZ Monica, een drinkwatermaatschappij zoals De Watergroep

Belangrijk

Een diepvriesgroentenproducent met 120 werknemers, een IT-dienstverlener met 60 werknemers die KMO’s beheert

Niet

De bakker om de hoek met 6 werknemers

Niet automatisch

Een gemeente, tenzij ze een activiteit uit de bijlagen uitvoert. Vlaanderen wil alle lokale besturen mee tegen 2030.

De rol van het CCB

Registratie

Organisaties registreren zich via **Safeonweb@Work**.

CSIRT

Via **CERT.be** ontvangt het CCB de meldingen en helpt het bij incidenten.

Toezicht

Inspecties en sancties, voor sommige sectoren samen met een sectorale overheid.

Zorgplicht

Passende maatregelen op basis van een **risicoanalyse**, met minstens:

- Risicoanalyse
- Incidentbehandeling
- Back-ups en continuïteit
- Toeleveringsketen
- Veilige ontwikkeling
- Cryptografie
- Toegangsbeheer
- MFA
- Opleiding personeel

Ook als je zelf niet onder NIS2 valt: een klant die dat wel doet, zal van jou als **leverancier** bewijs vragen.

BESTUURDERS ZIJN AANSPRAKELIJK

De directie moet de maatregelen **goedkeuren**, **opvolgen** en een **opleiding** volgen.

Doet ze dat niet, dan is ze **persoonlijk aansprakelijk**. Bij een essentiële entiteit kan het CCB zelfs een tijdelijk bestuursverbod opleggen.

Meldplicht: significant incident

Significant = de dienstverlening ernstig verstoord, grote financiële schade, of aanzienlijke schade voor anderen.

1. **24 uur**: vroegtijdige waarschuwing (*early warning*). Wat is er aan de hand, kwaad opzet, grensoverschrijdend?

→

2. **72 uur**: incidentmelding met een eerste inschatting van ernst en impact

→

3. **1 maand**: eindverslag met oorzaak en genomen maatregelen

Melden bij het CCB via **notif.safeonweb.be**. Patiëntgegevens gestolen? Dan **óók** een GDPR-melding bij de GBA.

Sancties

€ 10 miljoen

of **2%** van de wereldwijde jaaromzet voor een **essentiële** entiteit

€ 7 miljoen

of **1,4%** van de wereldwijde jaaromzet voor een **belangrijke** entiteit

Daarvoor: waarschuwingen, bindende instructies, termijnen om het op te lossen.

CyberFundamentals (CyFun®)

Het CCB-framework om concreet in orde te raken, gebaseerd op onder meer **NIST CSF** en **ISO 27001**.

1. **Small**: basismaatregelen voor kleine organisaties
2. **Basic**: de fundamenten voor iedereen
3. **Important**: bij een verhoogd risico
4. **Essential**: tegen de meest gevorderde aanvallers

CyFun of **ISO 27001** op het juiste niveau = **vermoeden van conformiteit**.

Deadlines voor essentiële entiteiten

18/04/2026

minstens een CyFun-verificatie **Basic** of **Important**, of een overeenkomst voor ISO 27001

18/04/2027

het uiteindelijke **doelniveau** gecertificeerd

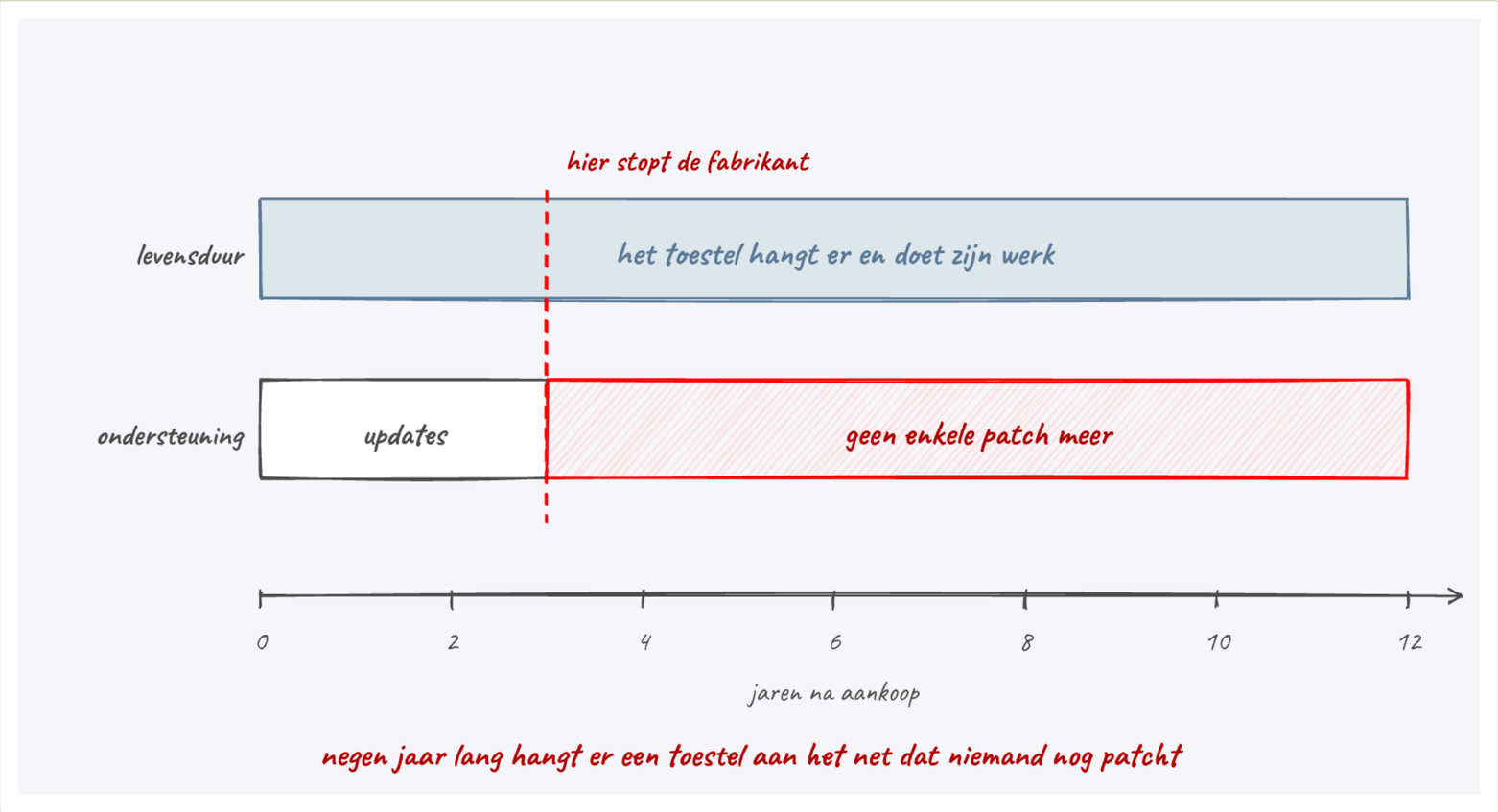
Belangrijke entiteiten moeten niet, maar het is de eenvoudigste manier om aan te tonen dat je in orde bent.

DEEL 3

Cyber Resilience Act

De fabrikant wordt verantwoordelijk voor de veiligheid van zijn **product**.

Het IoT-probleem, opnieuw



Een IoT-toestel gaat vlot tien jaar mee, de ondersteuning ervan zelden.

Default wachtwoorden, open poorten, geen updates: wie een onveilig toestel verkocht, riskeerde niets. De **CRA** (verordening EU 2024/2847) verandert dat.

Voor welke producten?

Producten met digitale elementen: hardware en software die met een toestel of netwerk verbonden kan worden. Van babyfoon tot besturingssysteem.

Belangrijk, klasse I

Wachtwoordmanagers, browsers, VPN’s, routers, besturingssystemen, slimme sloten en camera’s

Belangrijk, klasse II

Firewalls, inbraakdetectie, hypervisors, tamper-resistant microprocessoren

Kritiek

Smartcards, secure elements, HSM’s

Niet: medische hulpmiddelen, auto’s, luchtvaart, defensie, pure SaaS en niet-commerciële open source.

Wat moet de fabrikant doen?

- ✓ **Geen gekende kwetsbaarheden** bij het op de markt brengen
- ✓ **Secure by default**, met een reset naar die veilige toestand
- ✓ **Beperkt aanvalsoppervlak**: geen onnodige poorten en services
- ✓ Data beschermen (encryptie) en **minimaliseren**
- ✓ **Gratis security-updates**, waar mogelijk automatisch
- ✓ Een beleid om **kwetsbaarheden te laten melden** (*coordinated vulnerability disclosure*)

Voldoet het product? Dan brengt de fabrikant zelf een **CE-markering** aan. Bij gevoelige producten controleert eerst een erkende, onafhankelijke instantie mee.

Supportperiode en SBOM

Supportperiode

- Afgestemd op hoe lang het product gebruikt wordt
- **Minstens 5 jaar** (tenzij het product korter meegaat)
- Einddatum **vermeld bij aankoop**

vs

SBOM

- *Software Bill of Materials*: een **stuklijst** van alle componenten
- Machineleesbaar (bv. SPDX, CycloneDX)
- Nieuwe Log4Shell? In enkele minuten weet je welke producten getroffen zijn

MELDPLICHT SINDS 11 SEPTEMBER 2026

Fabrikanten melden **actief misbruikte kwetsbaarheden** en **ernstige incidenten** in hun product.

Via het **Single Reporting Platform** van ENISA, dat tegelijk het CSIRT (in België het CCB) verwittigt. **24 uur** early warning, **72 uur** melding, eindverslag **14 dagen** na de patch (kwetsbaarheid) of **1 maand** na de melding (ernstig incident). Ook voor producten die al op de markt waren.

Tijdlijn CRA

1. **10 december 2024**: de CRA treedt in werking
2. **11 juni 2026**: regels voor de beoordelingsinstanties
3. **11 september 2026**: meldplicht voor fabrikanten
4. **11 december 2027**: volledige toepassing en CE-markering

Boetes tot **€ 15 miljoen of 2,5%** van de wereldwijde jaaromzet.

Meldplichten naast elkaar

	GDPR	NIS2	CRA
Wat?	Datalek met persoonsgegevens	Significant incident	Misbruikte kwetsbaarheid of ernstig incident in een product
Wie?	Wie persoonsgegevens verwerkt	Essentiële en belangrijke entiteiten	Fabrikanten
Aan wie?	GBA (+ betrokkenen)	CCB (+ afnemers)	CSIRT/CCB en ENISA (+ gebruikers)
Termijnen	72 uur	24 u / 72 u / 1 maand	24 u / 72 u / 14 dagen na patch of 1 maand (incident)
Sinds	25/05/2018	18/10/2024	11/09/2026

Eén ransomware-aanval kan dus drie meldplichten tegelijk in gang zetten. Het **Digital Omnibus**-voorstel (2025) wil één Europees meldpunt, maar is nog geen wet.

Conclusie

- ✓ **GDPR** beschermt je persoonsgegevens, met boetes tot 4% van de omzet
- ✓ **NIS2** verplicht organisaties in kritieke sectoren tot een zorgplicht en een meldplicht binnen **24 uur**, met aansprakelijke bestuurders
- ✓ **CyFun** en **ISO 27001** zijn de manier om aan te tonen dat je in orde bent
- ✓ De **CRA** maakt fabrikanten verantwoordelijk voor veilige producten en jarenlange updates
- ✓ Een informaticus komt ze alle drie tegen: als ontwikkelaar, als werknemer en als bouwer van producten