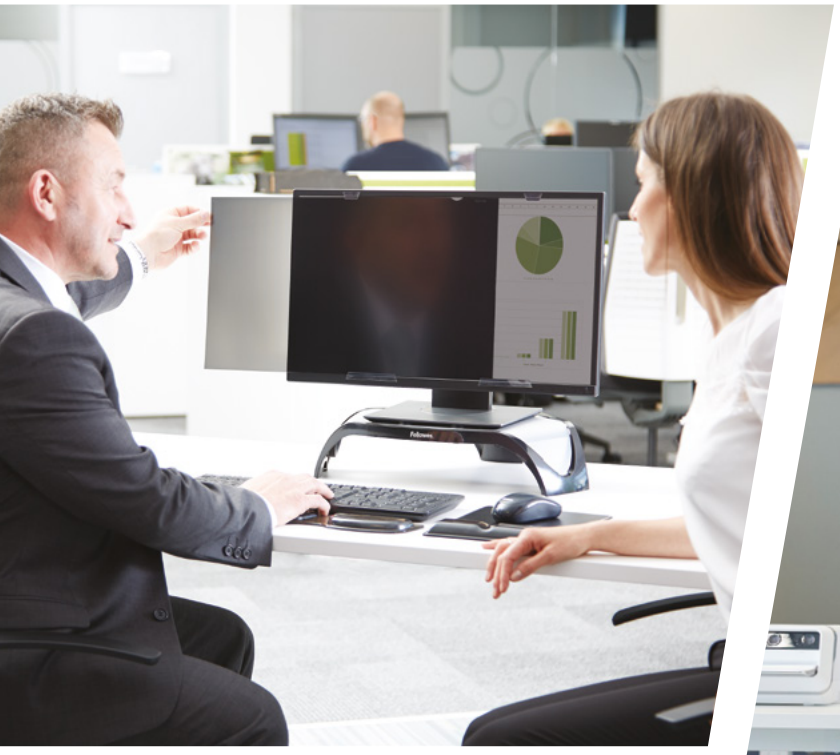
[STRENGTHEN YOUR SECURITY]

with **Fellowes**



*Begrijp **AVG** & **NIS-2** regelgeving en maak gegevensbescherming een onderdeel van je dagelijkse werk*

Fellowes®

INLEIDING

Waarom gegevensbescherming belangrijker is dan ooit

In een steeds meer verbonden wereld met cyberdreigingen en privacy risico's is gegevensbescherming niet langer optioneel. Het beschermen van je bedrijfsgegevens is essentieel en het naleven van privacywetgeving is belangrijker dan ooit.

Regelgeving zoals de AVG en de geüpdatete NIS-2-richtlijn verplichten bedrijven om gevoelige en persoonlijke gegevens op een verantwoorde manier te beschermen – zowel fysiek als digitaal. Niet-naleving kan leiden tot hoge boetes, reputatieschade en zelfs persoonlijke aansprakelijkheid van leidinggevenden.

Deze gids geeft een overzicht van beide regelgevingen, helpt je je verplichtingen te begrijpen en geeft handvatten om vol vertrouwen stappen te zetten richting compliance.

Versterk je beveiliging.
Bescherm je bedrijf.
Blijf compliant.

Wat zijn persoonsgegevens?

Persoonsgegevens zijn alle informatie over een levende persoon waarmee deze direct of indirect kan worden geïdentificeerd, zoals:

- **Naam**
- **Adres**
- **Burgerservicenummer / sociale zekerheidsnummer**
- **Beelden van CCTV-camera's**

Gegevensbescherming betekent het beschermen van zowel digitale als papieren informatie – een datalek kan immers in beide vormen plaatsvinden.

WAT IS NIS-2?

Cybersecurity in Europa versterken

De Netwerk- en Informatiebeveiligingsrichtlijn 2 (NIS-2) is de nieuwste EU-wetgeving om de cyberveiligheid en veerkracht van kritieke sectoren te verbeteren. Deze trad in 2023 in werking, en alle EU-lidstaten moeten deze uiterlijk oktober 2024 implementeren.

NIS-2 erkent dat moderne economieën afhankelijk zijn van digitale infrastructuur en dat verstoringen door cyberincidenten ernstige gevolgen kunnen hebben. Daarom geldt de richtlijn zowel voor essentiële als belangrijke organisaties.

Is NIS-2 van toepassing op jouw bedrijf?

Als jouw organisatie een sleutelrol speelt in de economie of samenleving, zelfs indirect, valt deze waarschijnlijk onder NIS-2. De richtlijn is van toepassing op producten en diensten die als “essentieel” of “belangrijk” zijn gecategoriseerd.

Essentiële organisaties:

- Energie
- Transport
- Digitale infrastructuur
- Banken
- Financiële markten
- Drinkwater
- ICT-beheer
- Publieke administratie
- Ruimtevaart
- Afvalwater
- Gezondheidszorg

Belangrijke organisaties:

- Post- en koeriersdiensten
- Afvalbeheer
- Productie
- Chemische productie
- Onderzoek
- Voedselproductie
- Digitale dienstverleners

De twee basisprincipes van NIS-2

Organisaties die onder NIS-2 vallen, moeten zowel preventieve maatregelen als responsmechanismen implementeren.

Zorgplicht (Duty of Care):
Organisaties moeten proportionele technische, operationele en organisatorische maatregelen nemen om digitale veiligheid en continuïteit te waarborgen. Dit omvat het beveiligen van IT-systemen, risicoanalyse, beheer van leveranciersrisico's en verantwoordelijkheid op managementniveau.

Meldplicht (Duty to Report):
Organisaties moeten de relevante nationale autoriteit op de hoogte stellen van significante incidenten. Grote verstoringen moeten binnen 24 uur gemeld worden, andere incidenten binnen 72 uur. Een gedetailleerd eindrapport moet binnen één maand worden ingediend.

Boetes bij niet-naleving:

Niet-naleving kan leiden tot ernstige financiële en operationele gevolgen:

€10 miljoen
of 2 % van de wereldwijde jaaromzet voor **essentiële organisaties**

€7 miljoen
of 1,4 % van de wereldwijde jaaromzet voor **belangrijke organisaties**

Bedrijfsleiders kunnen persoonlijk aansprakelijk worden gesteld, inclusief tijdelijke of permanente verbod op activiteiten in bepaalde sectoren.

Het verborgen risico: papieren datalekken

Hoewel NIS-2 zich richt op digitale veerkracht, mogen fysieke datarisico's niet worden genegeerd. Elk incident waarbij persoonsgegevens verloren gaan, gestolen worden of onjuist worden openbaar gemaakt, telt – inclusief papieren documenten die niet veilig worden vernietigd. Denk aan contracten in de afvalbak, spreadsheets op bureaus, HR-dossiers in onveilige kasten, of facturen in open recyclingbakken. Elk scenario kan leiden tot boetes en reputatieschade.

WAT IS AVG?

Persoonsgegevens beschermen

De Algemene Verordening Gegevensbescherming (AVG) regelt sinds 2018 gegevensbescherming in de EU en het VK. Ze zorgt ervoor dat persoonsgegevens op een wettelijke, transparante en veilige manier worden verwerkt.

De 6 principes van gegevensbescherming

Deze principes vormen de kern van iedere gegevensbeschermingsstrategie:

1. Wettige, eerlijke en transparante verwerking
2. Verzameling voor specifieke, expliciete en legitieme doeleinden, geen verwerking die daarmee in strijd is
3. Adequaat, relevant en beperkt tot het noodzakelijke
4. Juist en up-to-date; onjuistheden direct corrigeren of verwijderen
5. Niet langer bewaren dan noodzakelijk
6. Veilig verwerken

Wanneer moet een datalek gemeld worden?

Datalekken moeten binnen 72 uur aan de toezichthouder worden gemeld, in sommige gevallen ook aan betrokkenen.

Boetes bij niet-naleving:

Niet-naleving kan leiden tot zware financiële consequenties:

NIS-2 vs AVG

De verschillen begrijpen

Kort samengevat: zo verschillen de twee regelgevingen in één oogopslag:

ASPECT	NIS-2	AVG
Focus	Cybersecurity & digitale veerkracht in essentiële en belangrijke sectoren	Bescherming van persoonsgegevens (digitaal & papier) voor alle organisaties die EU/UK-burger gegevens verwerken
Toepassingsgebied	Essentiële & belangrijke organisaties (energie, transport, banken, gezondheid, digitale infrastructuur etc.)	Elke organisatie die persoonsgegevens verzamelt, opslaat of verwerkt
Kernprincipes	Zorgplicht & Meldplicht	Zes principes van gegevensbescherming (rechtmatigheid, doelbinding, minimalisatie, juistheid, bewaarbeperking, integriteit & vertrouwelijkheid)
Melden van incidenten	Autoriteiten binnen 24u (verstoring), 72u (andere gevallen)	Toezichthouder binnen 72u, soms ook betrokkenen
Boetes	Tot €10M of 2% (essentiële), tot €7M of 1,4% (belangrijke)	Tot €20M of 4% van wereldwijde omzet
Management-aansprakelijkheid	Bestuurders kunnen persoonlijk aansprakelijk zijn	Organisatie als geheel wordt beboet, verantwoordelijkheid kan DPO/manager betreffen

Praktische acties

Compliance versterken

Voor de meeste organisaties betekent naleving van NIS-2 en AVG een combinatie van duidelijk beleid, veilige technologie en dagelijks bewustzijn bij medewerkers.

1 Verplichtingen bevestigen

- [ ] Controleren of jouw organisatie als essentiële of belangrijke organisatie onder NIS-2 valt
- [ ] AVG-verplichtingen checken en begrijpen welke gegevens worden verwerkt en waarom

2 Beveiligingspraktijken versterken

- [ ] Firewalls, encryptie en incident-response-plannen implementeren en up-to-date houden
- [ ] Fysieke risico's niet negeren – controle over print-outs, archivering en veilige verwijdering

3 Meldprocedures definiëren

- [ ] Duidelijke escalatieroutes voor incidenten vastleggen
- [ ] Verantwoordelijkheid voor melding en documentatie toewijzen
- [ ] Team voorbereiden op strikte meldtermijnen (24–72 uur)

4 Medewerkers regelmatig trainen

- [ ] Gegevensbescherming onderdeel maken van de dagelijkse cultuur, niet alleen IT-beleid
- [ ] Digitale risico's (phishing, wachtwoordhygiëne) en papieren risico's (opslag, versnipperen) behandelen

5 Document lifecycle beheersen

- [ ] Vernietigingsbeleid voor verouderde papieren documenten implementeren
- [ ] Gevoelige documenten veilig bewaren tot vernietiging
- [ ] Alleen bewaren wat nodig is – archieven regelmatig controleren en verlopen documenten veilig vernietigen

Fellowes-oplossingen

Praktische tools om compliance te versterken

Van veilig versnipperen tot georganiseerde archivering en privacy filters helpen Fellowes-oplossingen je informatie in elke fase van de levenscyclus te beschermen en ondersteunen naleving van NIS-2 en AVG.

Uitdaging:

Datalekken door papieren documenten voorkomen

Oplossing:

Papiervernietigers – integreren in het documentbeleid verkleint het risico op datalekken. Vernietig overbodige kopieën zodat gevoelige gegevens niet kunnen worden ingezien of misbruikt.

Ontdek papierversnipperaars.

Uitdaging:

Fysieke documenten veilig en systematisch opslaan

Oplossing:

Archiveringsoplossingen – houd archieven op orde met duidelijk gelabelde BANKERS BOX®-producten voor veilig transport tussen locaties tot vernietiging.

Ontdek onze opslag- en organisatieoplossingen.

Uitdaging:

Bescherming van schermgegevens tegen nieuwsgierige blikken

Oplossing:

Oplossing: Privacy filters – voorkomen visuele datadiefstal op schermen, ideaal voor hybride werkplekken en gedeelde kantoren.

PrivaScreen™ verduisterende privacyfilters

Uitdaging:

Apparaten onderweg of in gedeelde ruimtes beveiligen

Oplossing:

Oplossing: Laptopbescherming – de Breyta™ twee-in-één afsluitbare laptoptas beschermt laptop, belangrijke documenten en accessoires en fungeert tevens als laptopverhoger.

Maak kennis met Breyta™

Gegevensbescherming is niet langer alleen een IT-verantwoordelijkheid.
Het is een organisatie brede verplichting. Door af te stemmen op AVG en NIS-2 en veilige document- en datapraktijken te integreren in het dagelijkse werk, kan je organisatie boetes vermijden, vertrouwen opbouwen en veerkrachtig blijven.

Maak gegevensbescherming een onderdeel van je dagelijkse werk.

Fellowes Brands™ | EEN FAMILIEBEDRIJF SINDS 1917

www.fellowes.com