# Rol informatieveiligheidsconsulent

Bij decreet vastgelegd

* [Besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer](https://overheid.vlaanderen.be/sites/default/files/eIB_documents/E_GOV_decreet_BVR_VEILIGHEID.pdf) [**http://vtc.corve.be/docs/E\_GOV\_decreet\_BVR\_VEILIGHEID.pdf**](http://vtc.corve.be/docs/E_GOV_decreet_BVR_VEILIGHEID.pdf)
* Ethische gedragscode voor veiligheidsconsulenten (Kruispuntbank voor Sociale Zekerheid)

[**https://www.ksz.fgov.be/binaries/documentation/nl/securite/ethgedrag.pdf**](https://www.ksz.fgov.be/binaries/documentation/nl/securite/ethgedrag.pdf)

* VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 27 april 2016

betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) <http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679>

# Informatieveiligheidsbeleid CLB

## Verantwoordelijkheden

Directie:

* Verantwoordelijkheid en aansprakelijkheid informatieveiligheid CLB
* Oprichten Informatieveiligheidscel (kunnen opgenomen worden in deze cel: Directie, aanspreekpunt IV, ICT-verantwoordelijke, kwaliteitscoördinator, interne preventieadviseur, personeelsverantwoordelijke)
* Aanduiden aanspreekpunt voor de Netoverstijgende Werkgroep Informatieveiligheid CLB (NWGIVCLB)

Informatieveiligheidscel:

* Initiëren informatieveiligheidsbeleid
* Uitvoeren van de beslissingen en toepassen van richtlijnen
* Kaderen informatieveiligheid binnen interne kwaliteitszorg
* Rapporteren aan veiligheidsconsulent en Inrichtend Bestuur

Aanspreekpunt:

* Is coördinerend lid van de Informatieveiligheidscel
* Optreden als aanspreekpunt voor de Netoverstijgende werkgroep informatieveiligheid CLB (NWGIVCLB)
* Neemt deel aan vormingen georganiseerd door de NWGVCLB

## Taken informatieveiligheidscel

* Opstellen en actualiseren van het informatieveiligheidsbeleid voor het CLB, vertrekkend vanuit een beschrijving van de huidige situatie
* Opstellen en bijhouden van register van verwerking van persoonsgegevens
* Verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen
* Uitvoeren van [risicoanalyse](http://www.vclb-koepel.be/beleid-organisatie/informatieveiligheid2/risicoanalyse3) inzake informatieveiligheidsbeleid
* Voorstellen beheersmaatregelen
* Uitwerken van veiligheidsplan
* Stimuleren van veiligheidsbewustzijn: verzorgen en coördineren van voorlichting en interne opleiding van personeel op gebied van informatiebeveiliging
* Toezicht houden op de implementatie en naleving van het informatieveiligheidsbeleid
* Registreren van veiligheidsincidenten en de remediëring
* Rapporteren aan de directie/inrichtend bestuur/informatieveiligheidsconsulent
* Onderhouden van interne en externe contacten binnen dit kader
* Op de hoogte blijven van nieuwe ontwikkelingen en wetgeving op gebied van informatiebeveiliging