



Provincie
Oost-Vlaanderen
Voor ieder van ons

Waarom informatieveiligheid

- Omdat het actueel is:

Aantal cyberincidenten in België is verdubbeld op één jaar tijd

7x meer incidenten dan in 2010

Dinsdag 10 maart 2015 — CERT.be, het federale cyber emergency team, publiceert vandaag zijn rapport met de resultaten van alle meldingen die de organisatie in 2014 mocht ontvangen. Meest opvallende resultaat: het aantal werkelijke cyberincidenten is meer dan verdubbeld ten opzichte van 2013. Er waren in 2014 gemiddeld 822 cyberincidenten per maand tegenover 339 in 2013. Ten opzichte van 2010 is dit zelfs een verzevenvoudiging.

Nieuw EU-agentschap voor cyberbeveiliging in de maak

De Europese Commissie presenteerde vandaag plannen om de digitale veiligheid te waarborgen. Ze zal een nieuw agentschap voor cyberbeveiliging ...

Russische hackers plunderden de rekening van bijna 1500 Belgen

02/11/15 om 12:17 - Bijgewerkt om 12:16
Bron: Moneytalk

Russische hackers hebben 4,6 miljoen euro buitgemaakt bij enkele Europese grootbanken. De criminelen hebben 1458 Belgische klanten van onder meer KBC en Belfius beroofd. Na jaren onderzoek heeft het Brusselse parket het clandestiene netwerk blootgelegd.

222
KEER GEDEELD



LEES LATER



Informatieveiligheid

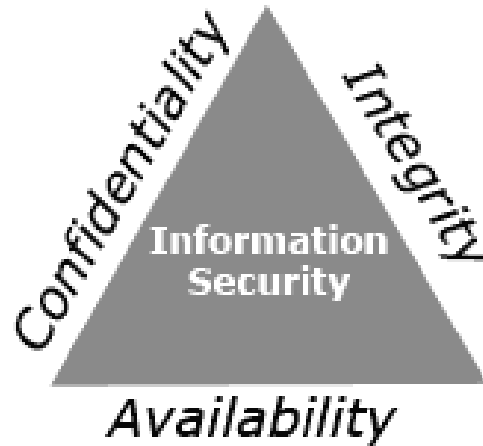
Maatregelen die ervoor zorgen
dat de betrouwbaarheid van informatie
behouden blijft, en incidenten worden
vermeden



Vertrouwelijkheid - bij de juiste mensen

Integriteit - de volledige en juiste informatie

Beschikbaarheid - op het juiste moment



Informatieveiligheid

- Achtergrond:
 - Elke burger heeft recht op gegevensbescherming (art. 8 EVRM)
 - Economisch? Dominantie internationale bedrijven.
 - Cybersecurity? Dominantie buitenlandse overheden

Privacywet (8/12/1992)

Uitgangspunten:

- **Finaliteit:** gerechtvaardigd doel
- **Proportionaliteit:** alleen relevante en noodzakelijke gegevens
- **Transparantie:** documenteren en openheid naar betrokkene
- **Termijn:** niet langer bewaren dan nodig
- ... en Beveiliging

PRIVACY

**IK HEB NIETS
TE VERBERGEN**

**MAAR DAT HOEVEN
ZE NIET TE WETEN**

Loesje

Postbus 1348
6801 DA Arnhem
www.loesje.nl

Algemene Verordening Gegevensbescherming

General Data Protection Regulation

= AVG: Algemene Verordening Gegevensbescherming
→ vervanging van de Privacywet 1992 maar dezelfde geest



Van toepassing vanaf 25 mei '18
= afdwingbaar
= verplichtingen nakomen

Verwerking

- Bewerking(en) m.b.t. persoonsgegevens:

Verzamelen

Vastleggen

Ordenen

Structureren

Opslaan

Bijwerken/wijzigen

Opvragen

Raadplegen

Gebruiken

Verstrekken dmv doorzending

Verspreiden

Aligneren/combineren

Afschermen

Wissen of vernietigen van gegevens

Verwerking

- Verwerkingsverantwoordelijke
 - Degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt
= bestuur/organisatie
- Verwerker
 - Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt
= leverancier

Privacycommissie-> Gegevensbeschermingsautoriteit.(GBA)



Bron: CBPL

Persoonsgegevens

- **Alle** informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene)
 - **direct** of **indirect** te identificeren, met name aan de hand van een **identifier**:
 - Naam
 - Identificatienummer
 - Locatiegegevens
 - Online identifier
 - Elementen kenmerkend voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit

Bijzondere persoonsgegevens (art.9)

- Ras/etnische afkomst
- Politieke opvattingen
- Religieuze/levensbeschouwelijke overtuigingen
- Vakbondslidmaatschap
- Genetische/medische gegevens
- Biometrische gegevens
- Seksuele voorkeur



Mogen (in principe) NIET verwerkt worden

Rechtmatigheid,
behoorlijkheid en
transparantie t.a.v. de
betrokkene

Doelbinding:

gegevens enkel verzameld voor duidelijk
omschreven en gerechtvaardigde
doeleinden en verwerkt volgens die
doeleinden

Minimale gegevensverwerking:

verwerking is ter zake dienend en beperkt
tot wat noodzakelijk is voor de opgegeven
doeleinden

Juistheid:

alle redelijke maatregelen worden
genomen om onjuiste gegevens onverwijld
te wissen of te rectificeren

Opslagbeperking:

niet langer bewaard dan nodig voor
doeleinden

Integriteit en vertrouwelijkheid:

passende technische en
organisatorische maatregelen om
gegevens te beschermen tegen
onopzettelijk verlies, vernietiging of
beschadiging

Essentiële wijziging GDPR: aantoonbaarheid (“accountability”): de
verwerkingsverantwoordelijke moet de naleving van de beginselen op ieder ogenblik kunnen
bewezen = bewijs dat maatregelen zijn genomen, dat verwerking beperkt is tot doeleinden, ...

Verplichtingen van de verantwoordelijke

- Treffen van organisatorische en technische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.
- A. Organisatorische
 - **Communicatie/transparantie**
 - Aanstelling FG (functionaris voor gegevensverwerking, veiligheidsconsulent, ...) (Art. 37, 38, 39)
 - **Keuze verwerker + verwerkingsovereenkomst (Art 28)**
 - **Houden van een intern register (Art 30)**
 - Effect beoordeling (DPIA) (Art 35)
 - Aansluiten bij goedgekeurde gedragscodes en certificering door GBA(Art 40-43)
- B. Technische (vooral ICT)
 - **Gegevens bescherming door ontwerp en door standaardinstellingen (Art 25)**
 - **Beveiliging van de verwerking (Art 32):**
 - **Melding inbreuken aan GBA en betrokkene (art 33,34)**

VOORBEREIDING OP NIEUWE PRIVACYWET IN 13 STAPPEN VAN WWW.PRIVACYCOMMISSION.BE

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de regels rond verwerking van persoonsgegevens. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.



2. REGISTER VAN VERWERKINGSACTIVITEITEN

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.



3. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de gegevensbeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.



4. COMMUNICATIE

Evalueer je bestaande privacyverklaring en bekijk deze in het licht van de AVG.



5. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.



6. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.



7. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.



8. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

9. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.



10. GEGEVENSLEKKEN

Voorzie adequate procedures om persoonlijke gegevenslekken op te sporen, te rapporteren en te onderzoeken.

11. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.



12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.



Wat is nieuw?

- Melden van datalekken aan de Gegevensbeschermingsautoriteit (GBA) (72u) en indien risico voor burger communicatieverplichting.
- DPIA (Data Protection Impact Assessment) bij projecten/risicovolle verwerkingen.
- Functionaris gegevensbescherming <-> informatieveiligheidsconsulent
- Privacy by design/default
- GBA krijgt tanden (boetes 4% omzet en tot €20 miljoen, inspectieopdracht, ...)

Bron: ICO en CBPL

1. Bewustmaking medewerkers



Phishing

Bierliefhebbers opgelet!

Dit is je kans om **1 jaar lang GRATIS BIER** te kunnen winnen. Je hoeft alleen maar te laten weten wat je favoriete bier is en waarom. Dit doe je door maar 3 vragen te beantwoorden. Simpel toch?

Geniet van de zomer met dit geweldige aanbod!

Beantwoordt de vragen op de volgende pagina

Ga nu verder!



75th Jarig Bestaan!

Deze maand vier IKEA haar 75 jarig bestaan!
Daarom een speciale actie voor IKEA klanten. Elke week, loten wij 100 klanten uit verschillende Vlaamse plaatsen. Dat betekent dat we in totaal maar liefst 400 klanten gelukkig gaan maken met een van de vele prijzen die wij klaar hebben liggen.

Deze week, is het jouw beurt karel@titeca.net!

Hoofdprijs € 500,- waardebon



U bent onze 1.000.000ste bezoeker! Dit is geen grapje!

Gefeliciteerd! Daarom bent u geselecteerd om een Apple product te winnen:

Apple iMac - Apple iPhone4 -
Apple iPad2

>> [Hier klikken](#) <<

Gefeliciteerd!

Win nu gratis boodschappen!



Delhaize waardebon

€ **150**
t.w.v.

DOE GRATIS MEE

Hoi karel@titeca.net,

We geven **gratis boodschappen** weg. En jij bent geselecteerd als een van de mogelijke winnaars! **Deze voucher ligt voor je klaar!** om je kans te verzilveren! En hopelijk doe jij binnenkort gratis boodschappen!

Heel veel plezier en succes!

Als het te mooi is om waar te zijn, is het meestal niet waar

2. Verwerkingsregister

Wat moet er in:

- Digitale toegangen
- Persoonsgegevens

Verplichtingen conform art. 30 GDPR

Naam en contactgegevens entiteit

Naam en contactgegevens DPO

Doeleinden verwerking

Categorieën betrokkenen

Categorieën verwerkte persoonsgegevens

Categorieën ontvangers: doorgifte naar andere overheden, derden, vzw's, landen binnen EU en buiten EU of internationale organisaties.

Buitenland = waarborgen t.a.v. elk doeleinde

Bewaartermijn

Technische en organisatorische beveiligingsmaatregelen

3. Interne en externe communicatie

- Intern:

- ICT-policy, deontologische codes
- Vertrouwelijkheidsclausules
- Sensibilisering



- Extern:

- Privacyverklaring website
- Klachten- en vragenformulier website

4/5. Rechten betrokkene

- **Recht op informatie**
- **Recht op inzage**
- **Recht op verbetering**



- [Recht om niet te worden onderworpen aan geautomatiseerde individuele beslissingen en profilering]
- [Recht op verwijdering (beperkt: archiefwet)]
- [Recht op gegevensoverdracht (bij wet geregeld)]
- [Recht op verzet tegen direct marketing (beperkt/nvt)]

4/5. Rechten betrokkene



Procedure(s) &
communicatiekanalen
inrichten om gevolg te geven
aan de rechten van de burger

4/5. Rechten betrokkene

Kopie verstrekken van verwerkte
persoonsgegevens

Huidige termijn: 45 dagen

Toekomst: 1 maand



Gratis, tenzij ongegrond of overmatig
(weigering of aanrekening mogelijk)

6. Grondslag verwerking

- Toestemming (intrekbaar)
- Contractuele relatie
- Wettelijke verplichting
- Noodzaak vrijwaring vitaal belang
- Algemeen belang of openbaar gezag
- Gerechtvaardigd belang verantwoordelijke

7.Toestemming

Expliciete toestemming nodig

- Geïnformeerd
- Ondubbelzinnig
- Vrij
- Specifiek



Geen vooraf aangevinkte vakjes

‘Opt-out’ even eenvoudig als de ‘opt-in’

7.Toestemming

Persoonsgegevens

- Inschrijvingen eetfestijn VZW



Verwerking enkel mogelijk indien:

- **Toestemming betrokkene (intrekbaar)**
- Noodzakelijk voor de uitvoering van de overeenkomst
- Noodzakelijk voor voldoen aan wettelijke verplichting van verwerkingsverantwoordelijke
- Nodig ter bescherming van de vitale belangen van de betrokkene
- Vervulling taak van algemeen belang of openbaar gezag verwerkingsverantwoordelijke
- Gerechtvaardigd belang

7.Toestemming

Persoonsgegevens

- Nieuwsbrief naar leden



Verwerking enkel mogelijk indien:

- Toestemming betrokkene (intrekbaar)
- Noodzakelijk voor de uitvoering van de overeenkomst
- Noodzakelijk voor voldoen aan wettelijke verplichting van verwerkingsverantwoordelijke
- Nodig ter bescherming van de vitale belangen van de betrokkene
- Vervulling taak van algemeen belang of openbaar gezag verwerkingsverantwoordelijke
- Gerechtvaardigd belang

7.Toestemming

Bijzondere persoonsgegevens

- Ras/etnische afkomst
- Politieke opvattingen
- Religieuze/levensbeschouwelijke overtuigingen
- Vakbondslidmaatschap
- Genetische/medische gegevens
- Biometrische gegevens
- Seksuele voorkeur



Mogen (in principe) NIET verwerkt worden

7.Toestemming

Bijzondere persoonsgegevens

Bv. VZW organiseert eetfestijn: allergieën?

Verwerking enkel mogelijk indien:

- **Toestemming (intrekbaar)**
- Nodig voor uitvoering overeenkomst
- Verwerking noodzakelijk op gebied van het arbeidsrecht en socialezekerheidsrecht
- De betrokkene maakt deze gegevens zelf openbaar
- Beoordeling van de arbeidsgeschiktheid van de werknemer of medische diagnoses
- Door stichting, vereniging of vzw die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is
- Nodig ter bescherming van de vitale belangen van de betrokkene



7.Toestemming

Procedures screenen op

- informeren over -en vragen van- toestemming
- documentering daarvan



- Zorg ervoor dat de betrokkene duidelijk ingelicht wordt over de verwerking waarvoor hij toestemming geeft
- Zorg ervoor dat het toestemmingsmechanisme in een werkelijke vrijwillige keuze voorziet en van nature een 'opt-in' situatie is
- Zorg voor een mechanisme waardoor de betrokkene zijn toestemming eenvoudig kan intrekken
- Zorg ervoor dat je je niet baseert op stilzwijgen of inactiviteit om toestemming te bekomen

8. Kinderen

Kinderen < 16 jaar = toestemming ouders/voogd nodig

België: waarschijnlijk < 13 jaar (Facebook)

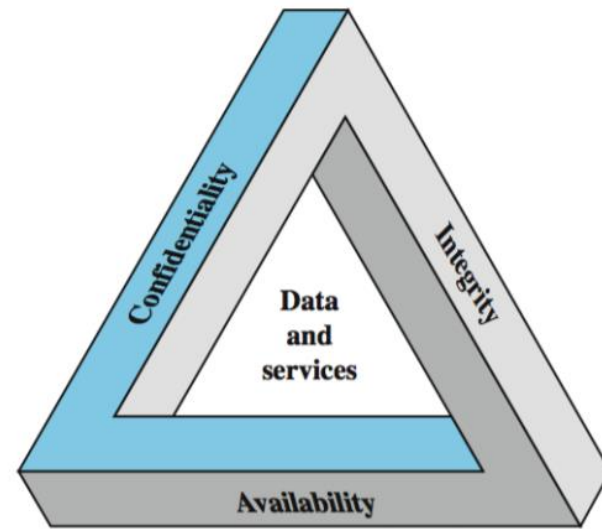


AGE OF CONSENT

G D P R

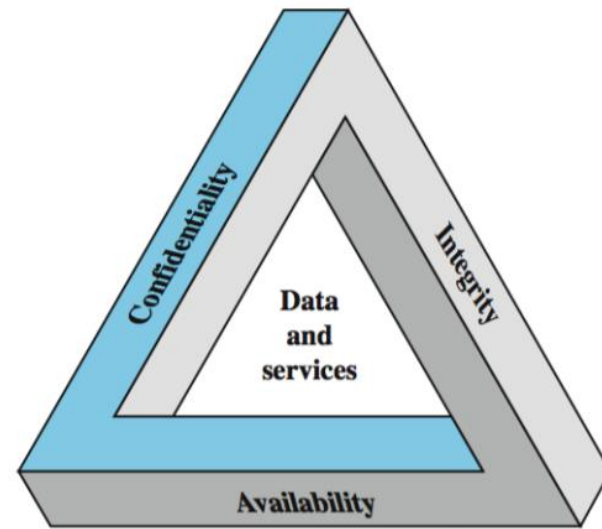
**DIFFERENT APPROACHES IN
DIFFERENT MEMBER STATES**

9. Datalek



- USB-stick verloren met persoonsgegevens
- verkeerd verzonden e-mail met persoonsgegevens
- dossier verloren
- open kasten of dossiers op bureau bij afwezigheid
- stroompanne
- (back-up) server down
- brand / wateroverlast in archief

9. Datalek



- inbraak
- diefstal laptop
- onrechtmatige inzage
- ongeautoriseerde toegang
- onrechtmatige opzoeken KSZ/RR
- malware besmetting / cryptolocker
- hacking

9. Datalek

Verplicht melden bij de **Privacycommissie** binnen 72 uur na ontdekking, wanneer een risico voor de rechten en vrijheden van personen

Mededelen aan de **betrokkene** wanneer waarschijnlijk een hoog risico voor zijn/haar rechten en vrijheden

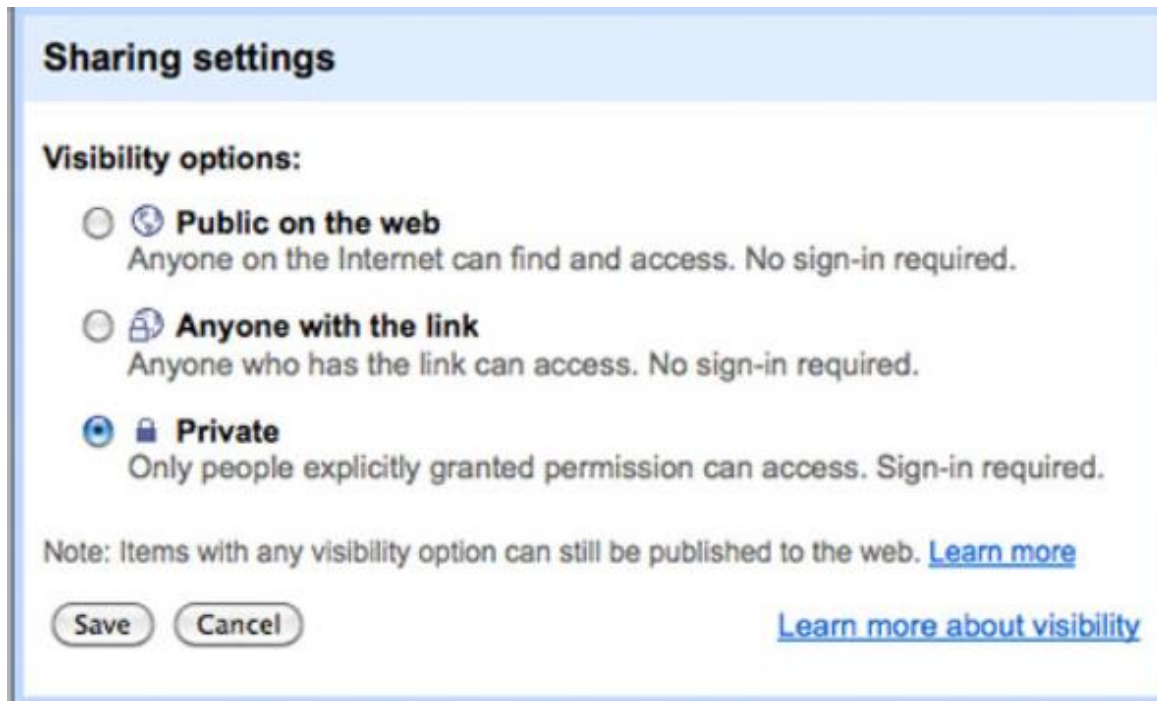
Eerste aanspreekpunt: ICT verantwoordelijke/DPO



- Zorg ervoor dat jouw medewerkers en personeel weten wat een inbreuk of data breach precies inhoudt
- Duid iemand aan die verantwoordelijk is voor het controleren en het rapporteren van de inbreuk (en)
- Zet een degelijk detectiesysteem op poten
- Bereid een template voor om inbreuken te melden

10. Privacy by design & by default

- By default/standaard instelling = maximale privacy
- By design/ontwerp = maximale privacy



Sharing settings

Visibility options:

- ☐ **Public on the web**
Anyone on the Internet can find and access. No sign-in required.
- ☐ **Anyone with the link**
Anyone who has the link can access. No sign-in required.
- ☒ **Private**
Only people explicitly granted permission can access. Sign-in required.

Note: Items with any visibility option can still be published to the web. [Learn more](#)

[Learn more about visibility](#)

[Save](#) [Cancel](#)

11. Functionaris Gegevensbescherming

Data Protection Officer
Informatieveiligheidsconsulent

Aanstellen tegen 25 mei 2018



Verplichting voor:

- verwerkingsverantwoordelijken (besturen, OCMW's, bedrijven)
- verwerkers (contractanten en leveranciers)

12. Internationaal (Art 44-50)

- Bij internationale dataverwerkingen
 - > Zijn er internationale afspraken? (Safe Harbour, ...)
 - > Zijn er bijkomende contactuele verplichtingen nodig.

13. Leveranciersrelaties



Evalueer bestaande overeenkomsten
en sluit verwerkingsovereenkomsten

Tips



- Wees waakzaam
- Verwacht vragen van burgers/klanten
- Verwacht controles
- Ken de risico's
- Bij incidenten/vragen:
frederik.dhondt@oost-vlaanderen.be

Meer weten

- <https://www.safeonweb.be/nl/home>
- <https://www.privacycommission.be/>
- <http://scwitch.be/toolkit/> voor
verwerkingsregister, verwerkingscontract
etc.

Vragen?



frederik.dhondt@oost-vlaanderen.be