



18/04/2018



ELIZA

Eerstelijns- en Interdisciplinaire Zorg Antwerpen
Universiteit Antwerpen

GDPR en AVG

‘Think Before You Save!’

Hilde Philips

huisarts, DPO, onderzoeker



Universiteit
Antwerpen

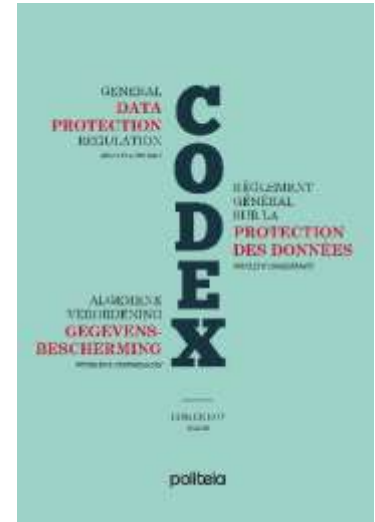
Bronvermelding

Codex: AVG/GDPR

<http://www.privacy-regulation.eu/>

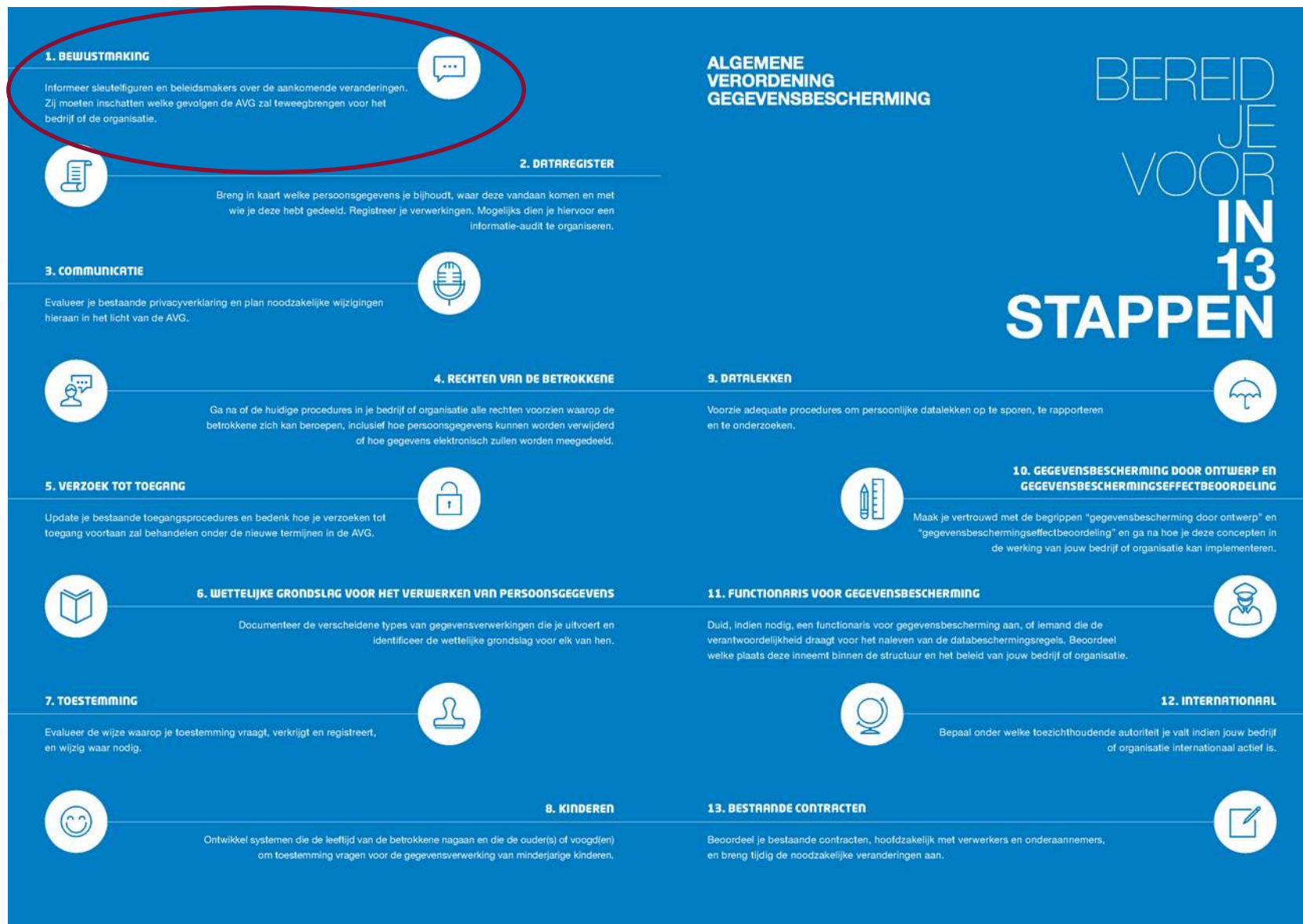
DPI: Data Protection Institute

<https://www.dp-institute.eu/nl/home/>



**Wie van u heeft al opleiding/presentatie
over de Algemene Verordening
Gegevensbescherming gevolgd?**





1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.



2.

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.



2. DATAREGISTER

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. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.



4. 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.

9. DATALEKKEN

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



5. VERZOEK TOT TOEGANG

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



10. 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.



6. 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.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

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



7. TOESTEMMING

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



12. INTERNATIONAAL

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



8. KINDEREN

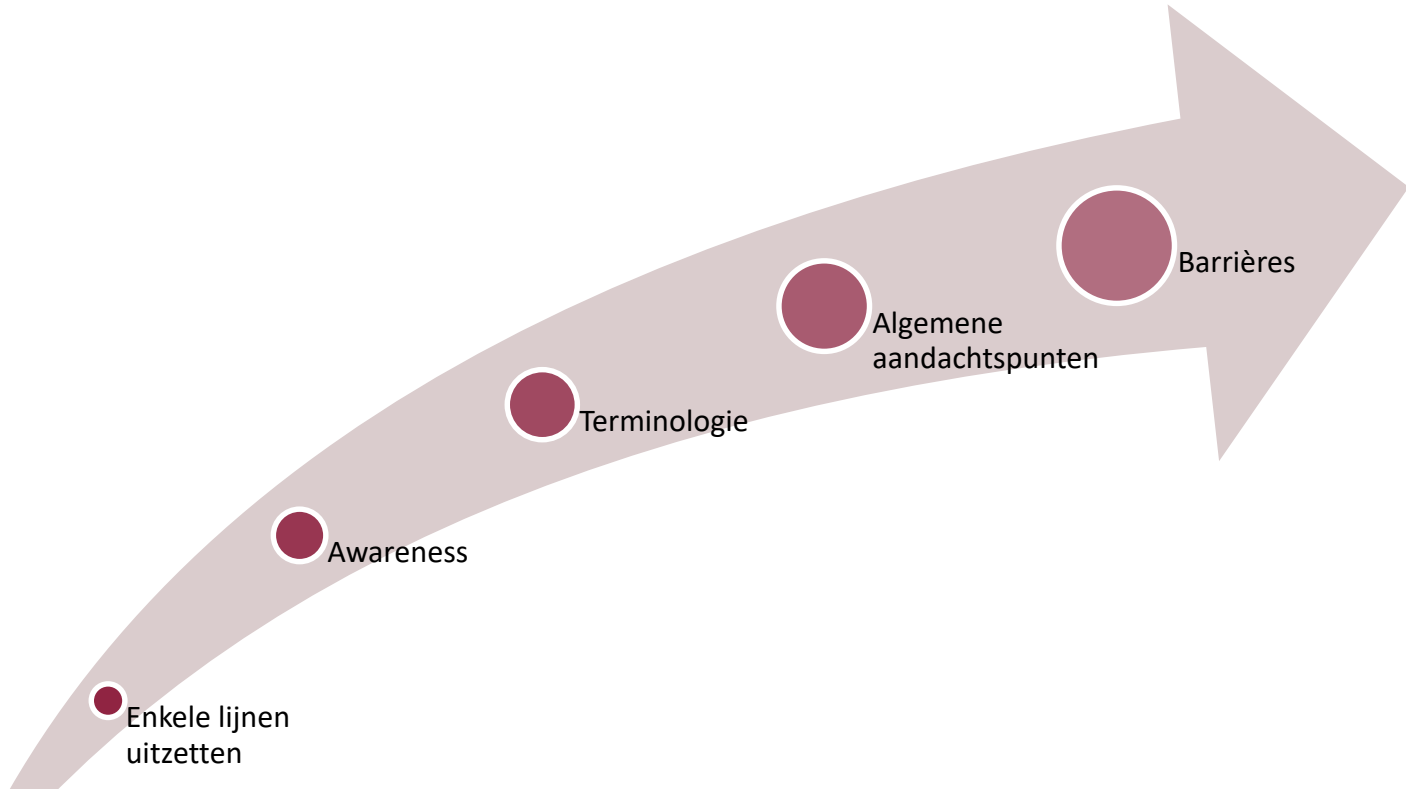
Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

13. BESTAANDE CONTRACTEN

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



Wat gaan we doen?



Correcte terminologie

GDPR: General Data Protection Regulation

AVG: Algemene Verordening Databescherming

= Europese wetgeving

Bepaalde aspecten worden door het Nationaal Recht bepaald (onder andere wetenschappelijk onderzoek)

Verwacht vandaag

niet

- Dat je straks **juridisch** alles zal weten
- Dat je **computertechisch** alles zal weten
- Dat je volledig onder de knie zal hebben wat je allemaal moet doen
- Dat we je kunnen garanderen dat je geen boetes zal krijgen ;-)

maar wel

- Dat je een overzicht hebt van wat er zal moeten gebeuren
- Je een aantal termen kent die van belang zijn
- Je een aantal struikelblokken binnen je eigen organisatie kan herkennen en bijsturen
- Je met een gerust hartje naar 25 mei toe kan leven 😊

Awareness seminar

- Bewustmaking
- Waarom is het nodig?
- Enkele begrippen
- Take home messages
- Eenvoudige maatregelen
- Wat wordt er verwacht tegen 25 mei?



Wat komt nu nog niet aan bod?



- Uitgebreide wetgeving
- Risico-analyse
- Technische beveiliging
- Procedure bij datalek
- Internationale uitwisseling
- Sancties

GDPR

Wat komt er
op ons af

- Wanneer?
- Voor wie?

De GDPR is er om de **burgers** te beschermen!

Iedereen van ons = 'data subject' of 'betrokkene'

=> transparantie is 'key'



- Wanneer?
- Voor wie?

⇒ 25 mei 2018:

- GDPR: General Data Protection Regulation
- AVG: Algemene Verordening Gegevensbescherming

⇒ Vanaf begin 2018:

- Bekendmaking groot publiek
- Sensibilisering van de burgers over hun rechten

- Wanneer?
- Voor wie?

Voor wie?

- Iedereen die persoonsgegevens verzamelt, bewerkt of bewaart op een 'structurele' manier
- Hoeft niet 'elektronisch' te zijn

Persoonsgegevens:

'Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon'

Het gaat dus over identificeerbaarheid en NIET alleen over privacy



Need to know



Nice to know

Nooit meer vergeten

Privacy

≠

Data protection

- Bescherming van de persoonlijke levenssfeer
- Bescherming van gegevens
- Dit is veel uitgebreider dan gegevens uit de persoonlijke levenssfeer van de betrokkene
- **Identificeerbaarheid** is hier het aandachtspunt

Allemaal onschuldige gegevens

Kolom 1				

Kolom 1	Kolom 2			

Kolom 1	Kolom 2	Kolom 3		

Kolom 1	Kolom 2	Kolom 3	Kolom 4	Kolom 5



Opgelet!

Het is niet omdat de gegevens momenteel geen gevaar op identificeerbaarheid betekenen of 'gevoelig' zijn, dat dit in de toekomst niet het geval kan zijn...

Een voorbeeld...



Welke gegevens heb ik nodig?

- Naam
- Leveringsadres
- Jaarlijkse meterstand
- Facturatiegegevens (indien $\neq$ van leveringsadres)

Welke gegevens heb ik nodig?

- Naam
- Leveringsadres
- Jaarlijkse meterstand
- Facturatiegegevens (indien $\neq$ van leveringsadres)



- Wens je domiciliëring?
- Wens je aanbiedingen te ontvangen ?
 - Zo ja?
 - Via mail
 - Via sms
- Wens je onze Nieuwsbrief te ontvangen?
 - Zo ja?
 - Per post?
 - Per mail?
 -



Slimme meters zijn wel slim...

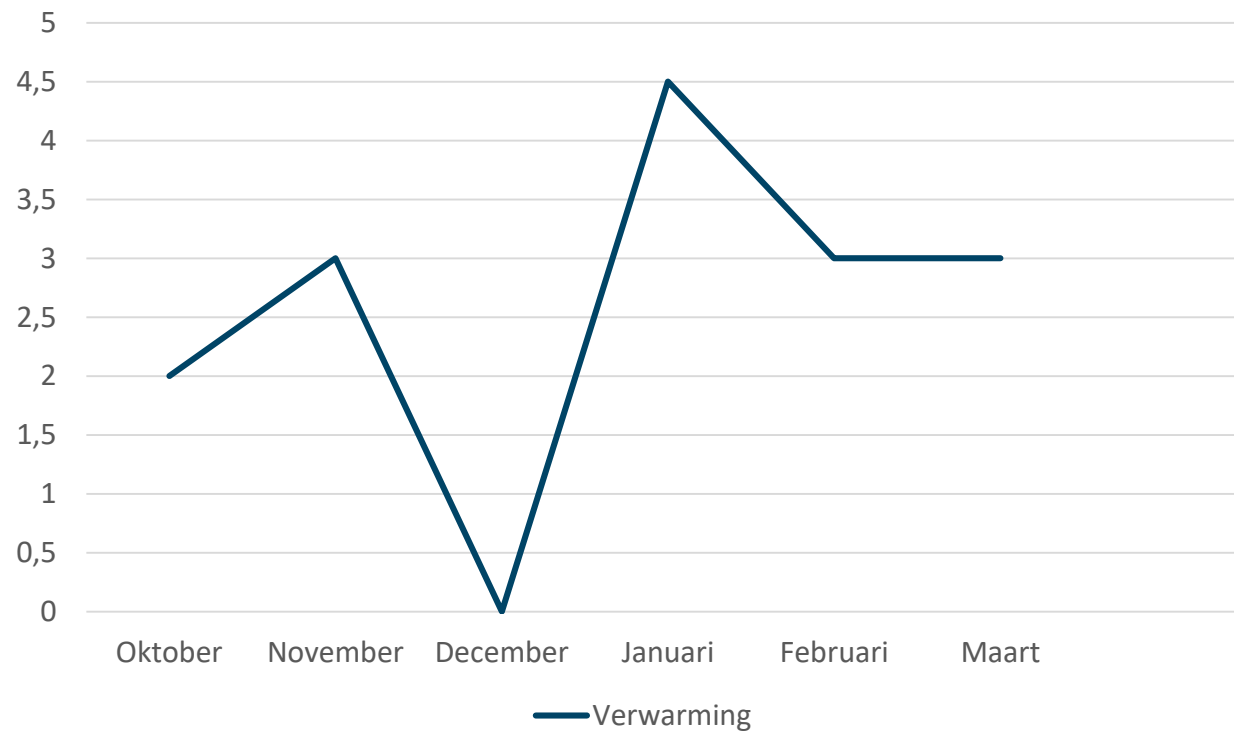
- Energieverbruik
- Jaarlijkse meterstand

En...

- Verbruik op elk moment
- Verloop van het verbruik
- Beïnvloedende factoren
- ...



Verwarming





Identificeerbaarheid!



Dit is het cruciale aandachtspunt!

Identificeerbaar? Let op!!!!

Anonieme gegevens

Nooit meer te herleiden tot een uniek identificeerbare persoon dus geen persoonsgegevens.

=> GDPR niet van toepassing

Gepseudonimiseerde of gecodeerde gegevens

Nog te herleiden tot een uniek identificeerbare persoon **door aanvullende gegevens.**

=> GDPR altijd van toepassing

NOOIT meer vergeten!



Need to know



Nice to know

Wat is jouw 'need to know'?

spelregels



- Verwerking: rechtmatig, behoorlijk en transparant
- Minimaal: beperkt tot het noodzakelijke! (Maar wel toereikend)
- Is het doel gerechtvaardigd? (doeleinden vastleggen)
- Gegevens moeten correct zijn!
- Bewaring: identificatie niet langer mogelijk dan noodzakelijk

Praktisch denken bij de implementatie

1. rechtmatig, behoorlijk, transparant
2. Minimaliseer

1. Informeer uw betrokkene ('privacyverklaring')
2. Indien geen persoonsgegevens nodig, doe het dan niet!

=> Aggregeer, wis...

3. Doel gerechtvaardigd?
4. Correcte gegevens?
5. Bewaring

3. Check in GDPR
4. Regelmatig checken
5. Zo mogelijk geanonimiseerd, niet langer dan nodig...

Bewaring!



Do's

Don'ts

- Geen persoonsgegevens via mail!!!!
- Geen persoonsgegevens op losse dragers!
- Laat deuren niet openstaan
- Bewaar geen data in kasten die toegankelijk zijn
- Zorg dat je scherm op slaapstand gaat na een tijdje inactiviteit

Bewaring!



Do's

Don'ts

- Vermeld telefonisch geen persoonsgegevens wanneer derden kunnen meeluisteren
- Zorg dat printen op afstand niet toegelaten is tenzij met persoonlijke aanmelding (idem faxapparaat)

Bewaring!



Do's

Don'ts

- Zorg dat patiënten u niet via mail, social media edm contacteren met gezondheidsvragen
- Check uw bronnen (kijk uit met telefoon!)
- Zorg dat er geen persoonsgegevens, gevoelige gegevens via websites uitgewisseld worden

Bewaring!



Do's

- Zorg voor toegangsbeveiliging
 - Registers (paswoorden, sleutels)
- Gebruik 'geijkte' kanalen voor gegevensuitwisseling (Zivver, Nictiz, Sophos...)
- Default settings printers edm
- Voorzie procedure bij datalek
- Maak van de ene datalek geen andere!

Don'ts

Bewaring!



Do's

Don'ts

Maar vooral:

- Overtuig iedereen op de werkvloer van het belang
- Breng bij iedere vergadering een GDPR item kort ter sprake



@santabanta.com



There is only one thing more painful than learning from experience, and that is not learning from experience.

Laurence J. Peter



NOOIT meer vergeten!



Need to know



Nice to know

Moeten we dit ook melden?



Datalek?

Wanneer spreken we van een datalek?

1. Wanneer iemand toegang tot gegevens (gehad) heeft waarvoor hij geen '**need to know**' heeft
=> meer gegevens ter beschikking dan noodzakelijk (vb. onzorgvuldige of niet correcte toegangsbeperking)
2. Wanneer iemand geen toegang tot gegevens heeft waarvoor hij wél een '**need to know**' heeft
=> noodzakelijke gegevens zijn niet/onvoldoende beschikbaar (vb. 'gijzeling' van data door ransomware)

Meldingsplicht voor datalek!

- Is nu al van toepassing!
- Elke datalek moet in principe gemeld worden aan de Privacy Commissie (volgens interne procedure vast te leggen wie wat onderneemt)
- Melding is verplicht binnen de 72u na vaststelling
- Inschatten van ernst:
 - Context van de data (DPC)
 - Risico op identificatie (EI)
 - Omstandigheden van de gegevenslek (CB)

$$SE \text{ (severity)} = DPC \times EI + CB$$



Bron: ENISA

'Recommendations for a methodology of the assessment of severity of personal data breaches'

Tijd voor wat terminologie...



Betrokkene

- Klant van een energiemeatschappij
- Om klant te zijn: aantal gegevens nodig!
 - Naam
 - Adres
 - Meterstanden (jaarlijks)

Doelstelling

- energie voorziening
- facturatie volgens verbruik (jaarlijkse meterstanden)

Betrokkene

- Klant van een energienetbeheerder
- Om klant te zijn: aantal gegevens nodig!
 - Naam
 - Adres
 - Meterstanden

Categorieën

Doelstelling

- energie voorziening
- facturatie volgens verbruik (jaarlijkse meterstanden)

Wettelijke
grondslag

Wat heeft dit nu allemaal te betekenen?

- 'Betrokkene' of 'data subject'
- Verantwoordelijke
- Verwerker

De **doelstelling** hangt samen met:

1. Categorieën van data (proportionaliteit, bewaartermijn,...)
2. De wettelijke grondslag obv dewelke data verwerkt worden
3. De rechten van de 'betrokkene'

Ik bestel een boek bij Bol.com

Wat hebben zij nodig?

- Welk boek wordt besteld?
- Wie heeft het besteld?
- Waar moet het geleverd worden?
- Aan wie moet er gefactureerd worden?

Grondslag?

‘Wettelijke verplichting’

Het zijn de minimale gegevens die noodzakelijk zijn om aan het contract of de overeenkomst te kunnen voldoen.



Bestelling is klaar...mijn boek wordt geleverd

Grondslag?

‘Wettelijke verplichting’

Het zijn de minimale gegevens die noodzakelijk zijn om aan het contract of de overeenkomst te kunnen voldoen.

Mijn rechten?

Zijn afhankelijk van de grondslag waarop de gegevens verwerkt worden.

Bij ‘wettelijke verplichting’ kan je bvb. geen recht op ‘wissen’ uitoefenen.

Andere wetten blijven geldig!

- Bij voorbeeld hoe lang een factuur bewaard moet worden?
- Overeenkomsten die vastgelegd zijn in contracten
- CAO's
- Wettelijke termijn om onderzoeksgegevens te bewaren
- Wettelijke termijn om gezondheidsgegevens te bewaren
-

Welke terminologie hebben we ondertussen gebruikt?

1. Betrokkene
2. Doelstelling
3. Categorieën
4. Grondslag

Betrokkene

= onderwerp van de ‘persoonsgegevens’

Alle informatie over een geïdentificeerde of identificeerbare persoon (“de betrokkene” of het “data-subject”)

- Direct of indirect identificeerbaar
- Naam, identificatienummer, locatiegegevens, IP adres...

Doelstelling

- Reden waarom gegevens verzameld, bewaard, verwerkt worden
- Welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden
- Mogen dus niet verder op een met die doeleinden onverenigbare wijze worden verwerkt

Categorieën

- Anonieme gegevens (vallen niet onder de GDPR)
- Naam, adres, IP adres, locatie... (persoonsgegevens, dus GDPR van toepassing)
- Verwerking van persoonsgegevens van bijzondere categorieën = verboden!

=> Meestal gebaseerd op de wet van de discriminatie

Bijzondere categorieën?



- Ras of ethnische afkomst
- Politieke opvattingen
- Religieuze of levensbeschouwelijke overtuigingen
- Lidmaatschap van een vakbond
- Genetische gegevens/biometrische gegevens met oog op unieke identificatie
- Gezondheidsgegevens
- Gegevens seksueel gedrag of seksuele geaardheid
- Strafrechtelijke en strafbare feiten

Gezondheidsgegevens

Maken deel uit van de categorie 'gevoelige persoonsgegevens' en mogen in principe niet verwerkt worden (artikel 9)
... tenzij omwille van bijzondere redenen!

Voor zorgverleners is volgende uitzondering van toepassing:

'(h) De verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen;'

Verder stelt de Europese regelgeving dat de verwerking van gezondheidsgegevens toegelaten is indien deze verwerkt worden door een beroepsgroep die onder het beroepsgeheim valt (artikel 9, lid 3)

Stel een privacy verklaring op

Situeer het wettelijk kader en leg de maatregelen uit die worden genomen om de gegevens te beschermen en lekken te voorkomen

Een privacyverklaring maakt duidelijk hoe er op een verantwoorde wijze met persoonsgegevens van patiënten wordt omgegaan

Deze kan in de wachtkamer gehangen worden of op de website geplaatst.

Grondslagen

= rechtmatigheid van de verwerking

Grondslagen

- Toestemming
- Overeenkomst
- Wettelijke verplichting
- Vitaal belang
- Algemeen belang/Openbaar gezag
- Gerechtvaardigd belang

Grondslagen

- Overeenkomst
- Wettelijke verplichting
- Vitaal belang
- Algemeen belang/Openbaar gezag
- Gerechtvaardigd belang
- **Toestemming**

De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij betrokkene partij is, of om op verzoek van betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen



De verwerking is noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust

=> Moet nationaal of Unierechtelijk zijn

Vitaal belang

Grondslagen

Verwerking is noodzakelijk om de vitale belangen van betrokkene of van een andere natuurlijke persoon te beschermen

Verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen

Ik wil mijn pakje
kunnen volgen!

Grondslagen

- Andere gegevens nodig
- GSM numm
- E-m



Gerechtvaardigd belang

⇒ 'wettelijke
plichting'

⇒ Andere grondslag
nodig!

⇒ Gevolg: andere rechten
die betrokkene kan
uitoefenen!

Design van de website/databank dient hierop voorzien te zijn!

Data protection by design!

Vb. Ticket bestellen bij NMBS online...

« Terug **Gegevens betaling →**

Gegevens betaler (* = verplichte velden)

Geslacht: * ☐ Man ☐ Vrouw

Voornaam: * Familienaam: *

E-mailadres: *

Betalingsmethode

Krediet-/Debetkaart :

☐ Mastercard ☐ Bancontact/Mister Cash ☐ BNP Paribas Fortis ☐ American Express ☐ Visa

Thuisbankieren :

☐ ING ☐ Belfius ☐ KBC ☐ CBC

☐ Ik ga akkoord met de verkoopvoorwaarden en de [vervoersvoorwaarden](#)

☐ Ontvang onze nieuwsbrief en blijf op de hoogte

(We verwerken uw persoonlijke gegevens. [Klik hier voor ons privacybeleid.](#))

« Terug **Gegevens betaling →**

= “elke vrije, specifieke, op informatie berustende en ondubbelzinnige, wilsuiting waarmee de betrokkene, door middel van hetzij een, verklaring, hetzij een ondubbelzinnige actieve handeling, aanvaardt dat, hem betreffende persoonsgegevens worden verwerkt”

I'M EXERCISING MY RIGHT
TO BE FORGOTTEN

SORRY, WHO ARE
YOU AGAIN?



Royston
roystoncartoons.com

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.



ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

2. DATAREGISTER



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. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.



4. 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.



9. DATALEKKEN

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



5. VERZOEK TOT TOEGANG

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



10. 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.



6. 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.



11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

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



7. TOESTEMMING

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



12. INTERNATIONAAL

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



8. 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.



13. BESTAANDE CONTRACTEN

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



Barrières

5 dooddoeners:

1. Wie zou er nu geïnteresseerd zijn in onze data?
2. Als ze onze data per se willen hebben, kunnen we dat toch niet beletten
3. De mensen zetten zelf heel hun leven op facebook
4. Privacy is enkel belangrijk voor mensen die van alles mispeuteren
5. We hebben het altijd al zo gedaan

Bron: Joris De Geyndt, 21 maart 2017



Eenvoudige adviezen



- Gebruik gezond verstand
- Indien geen persoonsgegevens (meer) nodig => wissen
- Geen (onbeveiligde) losse dragers
- Fysieke bescherming is N°1

Eenvoudige adviezen



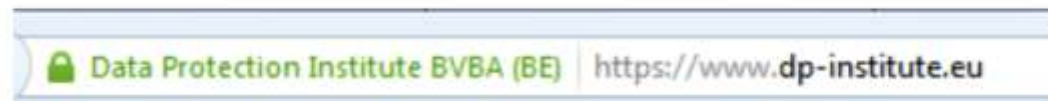
- Voorkom datalek of leer ervan
- Houd een 'intern register' bij van datalekken die je gehad hebt, noteer ook de oplossingen die je geïmplementeerd hebt
- Gebruik enkel beveiligde websites of programma's om persoonsgegevens te delen (enkel zo nodig)

https!

Voorbeeld van toepassing: SSL

- HTTPS: Hyper Text Transfer Protocol Secure
- HTTP verkeer dat verloopt over een beveiligde verbinding
- Verkeer dat via HTTPS is versleuteld en kan niet worden gelezen als het wordt onderschept
- Hoe herken je https?

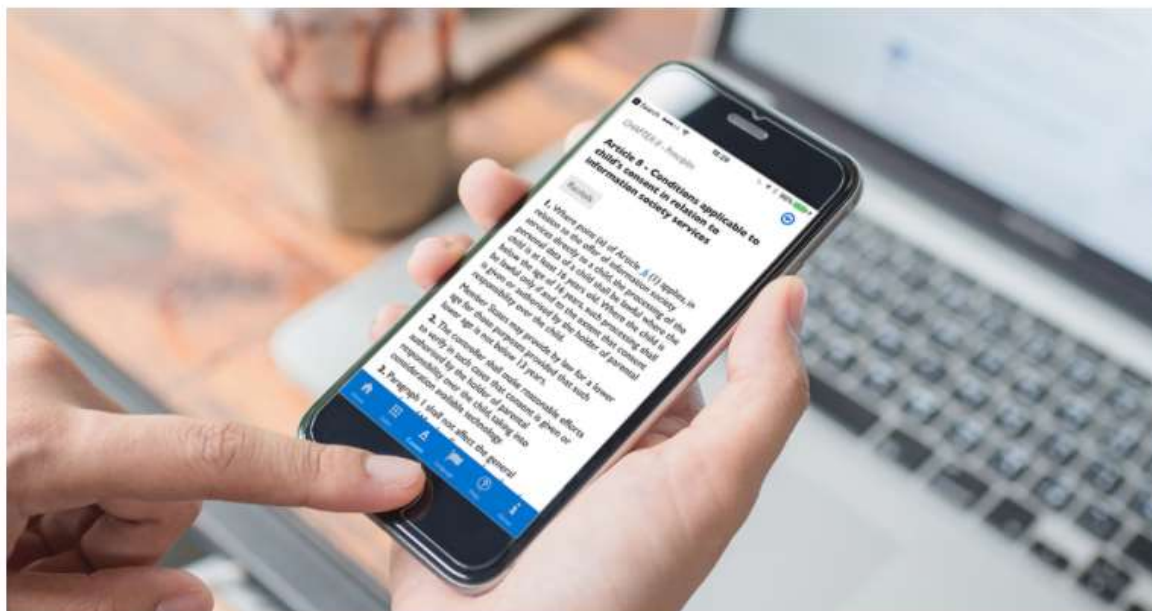
Safari →



Firefox →



EXPLORE GDPR: GET THE MOBILE APP

[HOME](#) [BACKGROUND](#) [KEY CHANGES](#) [ACTIONS TO TAKE](#) [HOW WE CAN HELP](#) [RESOURCES](#) [TEAM](#) [EVENTS](#) [RELATED INSIGHTS](#)
[e-mail](#) | [+ Delen](#)


The EU General Data Protection Regulation, which comes into force in May 2018, will introduce some of the most stringent data protection laws in the world. It is vital for anyone working with customer data to be familiar with its contents.

VERWANTE SECTOREN

[Technologie](#)

VERWANTE DIENSTEN

[Intellectual Property and Technology](#)

VERWANTE SITES

[Data Protection Handbook](#)

Deze website
functionaliteit
deze website v
impliciet in me
website. Meer

Tracking my cookies?

**They will never get my
recipe!**

