



GDPR op maat van arts én apotheker

EEN SAMENWERKING VAN



AGENDA

DEEL 1

GDPR & AVG: 'Think Before You Save!'

Dr. Hilde Philips

DEEL 2

GDPR in uw praktijk: Hoe starten? Concrete casussen

*Elfi Goesaert
Eef Dreesen*

SLOT

Vragenronde



DEEL 1

GDPR & AVG: 'Think Before You Save!'

Dr. Hilde Philips

Huisarts, DPO, onderzoeker



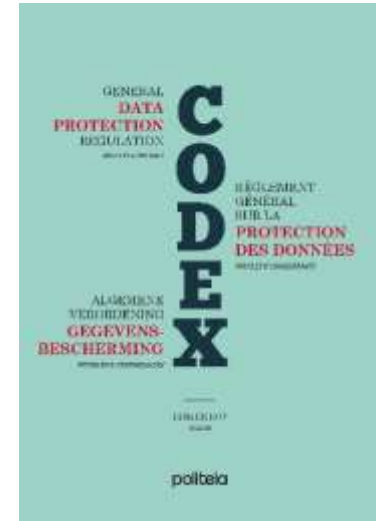
BRONVERMELDING

CODEX: AVG / GDPR

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

DPI: Data Protection Institute

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





**Wie van u heeft al
presentatie gevolgd over
de **A**lgemene **V**erordening
Gegevensbescherming?**

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.



ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

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.



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.



7. TOESTEMMING

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



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.



9. DATALEKKEN

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



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.



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.



12. INTERNATIONAAL

Bepaal onder welke toezichhoudende 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.



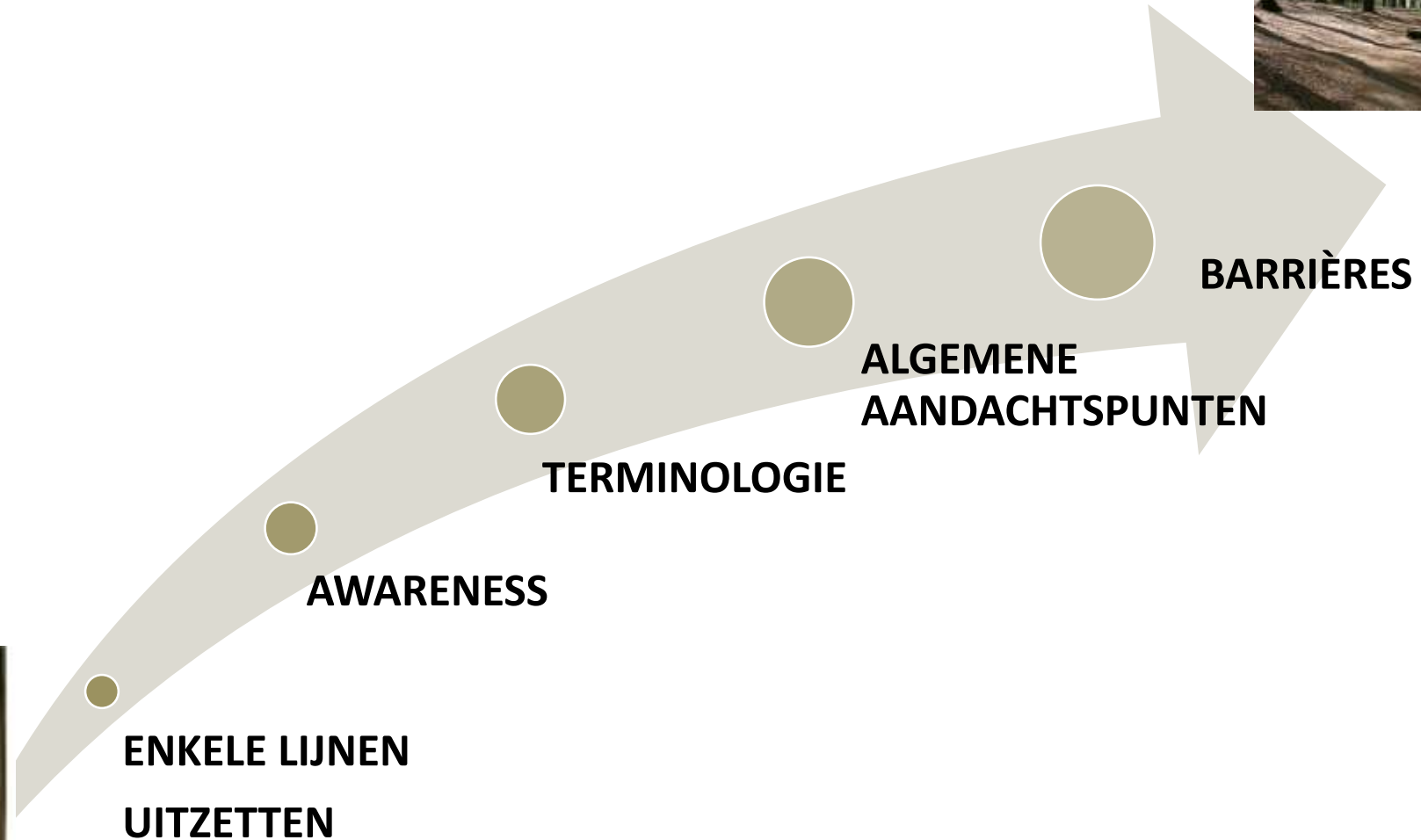
Stappenplan Frank
Robben: Privacy
Commissie

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.



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 (o.a. wetenschappelijk onderzoek)

Verwacht vandaag

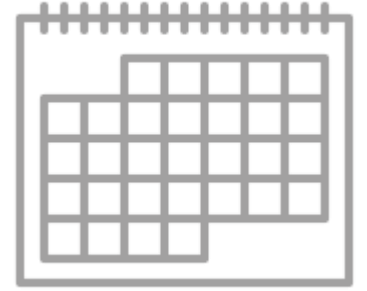
niet

- Dat je straks **juridisch** alles zal weten
- Dat je **computertechnisch** 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 😊

Wat komt er op ons af?



WANNEER?

⇒ **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

Wat komt er op ons af?



VOOR WIE?

- > De GDPR is er om de **burgers** te beschermen!
- > Iedereen van ons = 'data subject' of 'betrokkene'
- > => transparantie is 'key'

Wat komt er op ons af?



WIE MOET ERMEE REKENING HOUDEN?

- > 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

- Bescherming van de persoonlijke levenssfeer

≠

DATA PROTECTION

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

Allemaal onschuldige gegevens

[illegible]

[illegible]

[illegible]

[illegible]

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 ≠ 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?



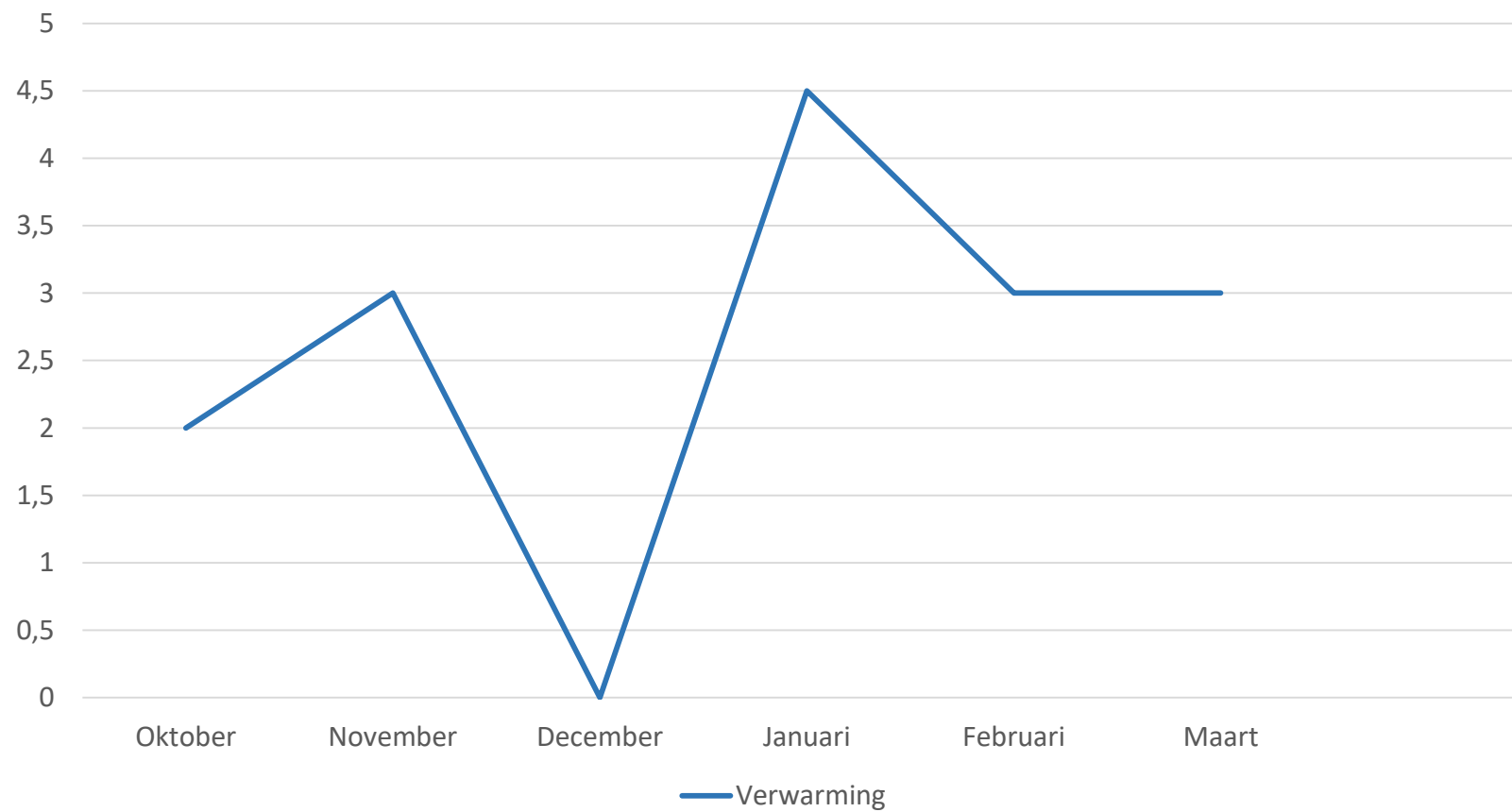
Slimme meters zijn wel slim...

- > 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

Praktisch denken bij de implementatie

1. Rechtmatig, behoorlijk, transparant → Informeer uw betrokkene ('privacyverklaring')
2. Minimaliseer → Indien geen persoonsgegevens nodig: doe het dan niet!
=> Aggregeer, wis, ...
3. Doel gerechtvaardigd? → Check in GDPR
4. Correcte gegevens? → Regelmatig checken
5. Bewaring → Zo mogelijk geanonimiseerd, niet langer dan nodig...



@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

Datalek?



Wanneer spreken we van een datalek?

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



Meldingsplicht voor datalek!

- > Is nu al van toepassing
- > Elk datalek moet 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

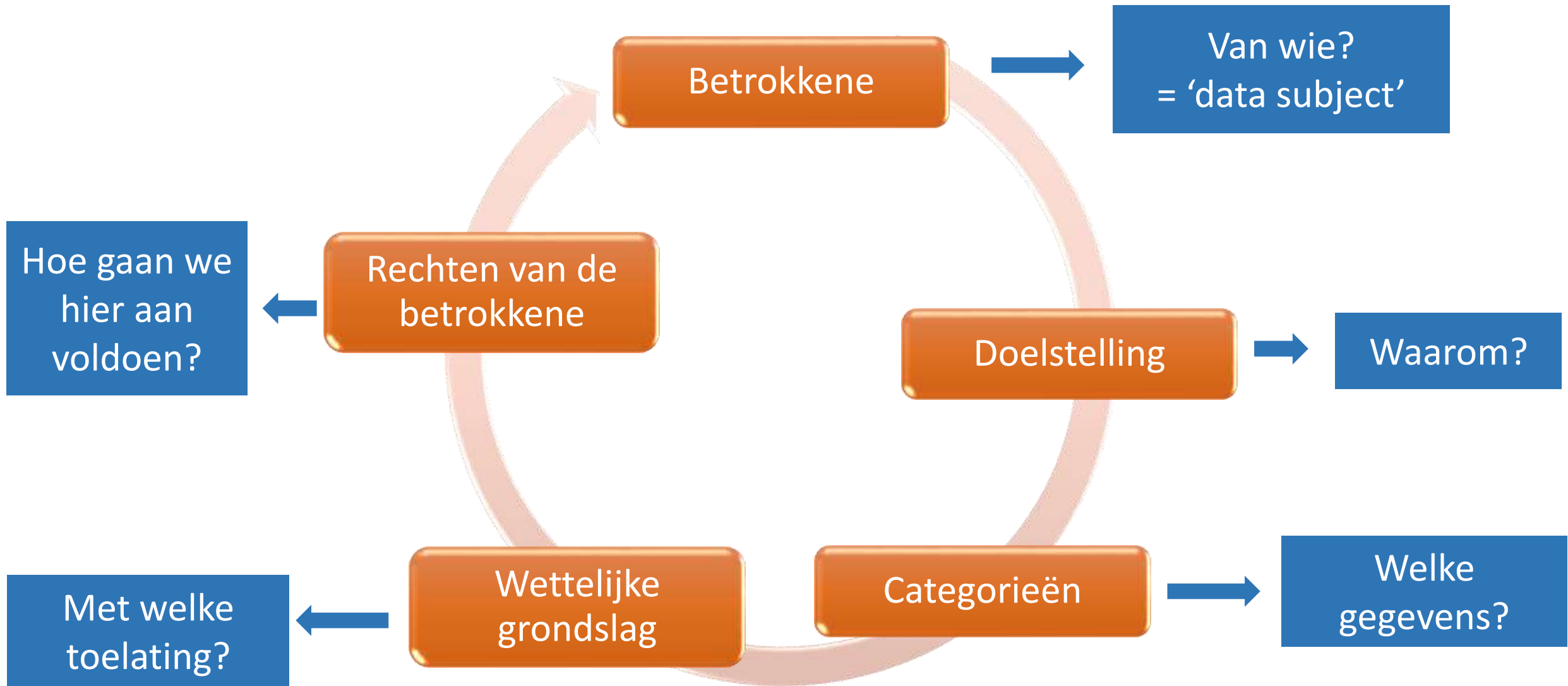


Bron: ENISA

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

Tijd voor wat terminologie...





Betrokkene

Klant van een energiemaatschappij

Om klant te zijn: aantal gegevens nodig

- Naam
- Adres
- Meterstanden

Doelstelling

Energievoorziening

Facturatie volgens verbruik (jaarlijkse meterstanden)

Betrokkene

Klant van een energiemaatschappij

Om klant te zijn: aantal gegevens nodig

- Naam
- Adres
- Meterstanden



Categorieën

Doelstelling

Energievoorziening

Facturatie volgens verbruik (jaarlijkse meterstanden)



Wettelijke
grondslag



Overeenkomst

Wat heeft dit nu allemaal te betekenen?

- > (Verwerkings)verantwoordelijke
 - > Verwerker
 - > 'Betrokkene' of 'data subject'
-
1. Verschillende **categorieën** van data (proportionaliteit, bewaartermijn,...)
 2. Deze worden verwerkt met een bepaalde **doelstelling**
 3. De **wettelijke grondslag** obv dewelke data verwerkt worden
 4. De **rechten** van de 'betrokkene'

Ik registreer mijn SLM kaart bij mijn provider

Wat hebben zij nodig?

- > Mobiel telefoonnummer
- > Naam
- > Facturatiegegevens

Grondslag?

- > 'Wettelijke verplichting'
- > Het zijn de minimale gegevens die noodzakelijk zijn om aan het contract of de overeenkomst te kunnen voldoen.



Ik bestel een boek bij Bol.com

Wat ligt contractueel vast?

- > Bestelling
- > Facturatiegegevens
- > Betalingsgegevens
- > Eventueel track and trace?

Grondslag?

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



Grondslagen hangen samen met rechten van de betrokkene..

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 bv. geen recht op 'wissen' uitoefenen.

Grondslagen hangen samen met rechten van de betrokkene..

Grondslag?

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

Mijn rechten

- > Recht van wissen is van toepassing
- > Databank dient dus opgebouwd te zijn zodat er ook tegemoetgekomen kan worden aan dit recht ('dataprotection by design')

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
- > Wetgeving volksgezondheid, RIZIV
- >

Welke terminologie hebben we ondertussen gebruikt?



BETROKKENE



CATEGORIEËN



DOELSTELLING



WETTELIJKE 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

- [illegible]

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;'*

Gezondheidsgegevens



- > 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)

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**

Grondslagen: Overeenkomst



- > 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



Grondslagen: Wettelijke verplichting



- > De verwerking is noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust
- > => Moet nationaal of Unierechtelijk zijn

Grondslagen: Vitaal belang



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

Grondslagen: Algemeen belang/ Openbaar gezag



- > 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!



Gerechtvaardigd belang

- > Andere gegevens nodig
- > GSM nummer?
- > E-mailadres?

- ⇒ Valt buiten 'wettelijke verplichting' en 'overeenkomst'
- ⇒ **Andere grondslag** nodig!
- ⇒ Gevolg: **andere rechten** die betrokkene kan uitoefenen!

Grondslagen: Toestemming



- > = “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?



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.



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.



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.



7. TOESTEMMING

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



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.



ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

9. DATALEKKEN

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



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.



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.



12. INTERNATIONAAL

Bepaal onder welke toezichhoudende 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.



Stappenplan Frank
Robben: Privacy
Commissie

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





OVER ONS KANTOREN NEWS WERKEN BIJ ONS

MENSEN SECTOREN DIENSTEN ACHTERGROND 

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



VERWANTE SECTOREN

[Technologie](#)

VERWANTE DIENSTEN

[Intellectual Property and Technology](#)

VERWANTE SITES

[Data Protection Handbook](#)

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.

Deze website functionaliteit deze website impliciet in me website. Meer

Tracking my cookies?

**They will never get my
recipe!**