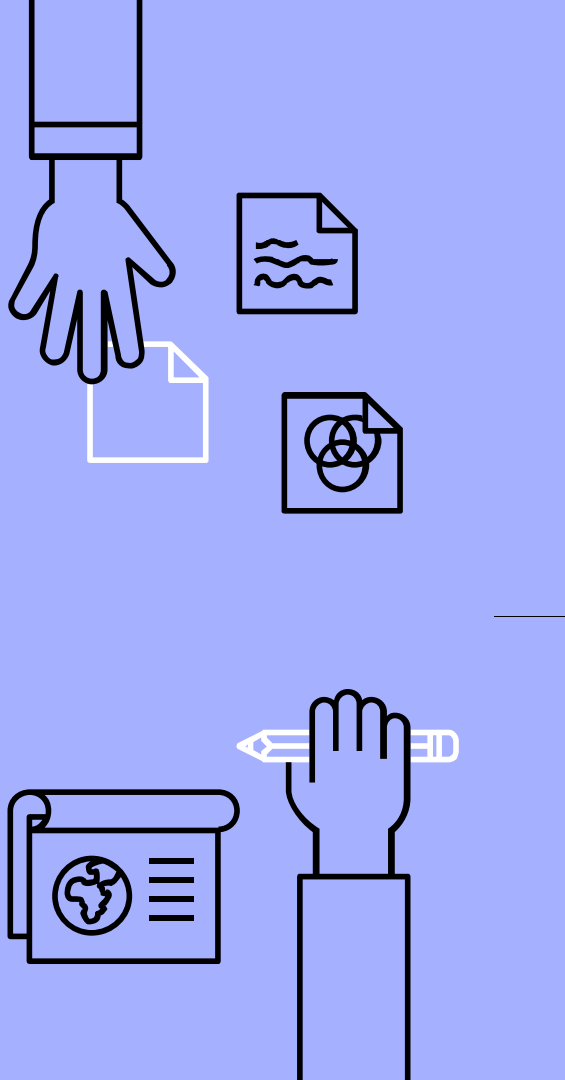
GDPR in een notendop

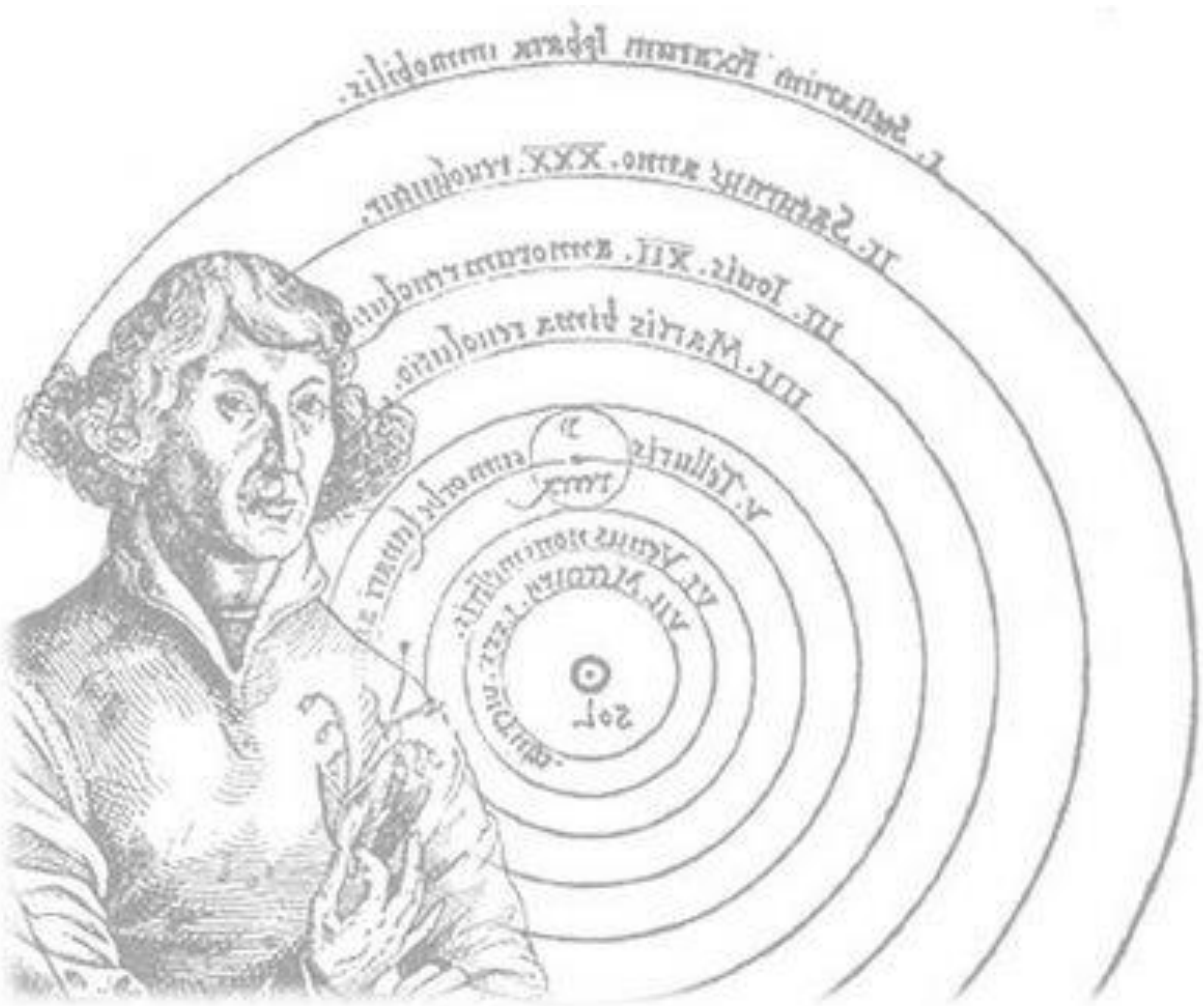
Wie is wie?

Mark Meerten – Smile@IT

mark@smileatit.be
0498/163.425
ICT Business Consultant
Certified DPO

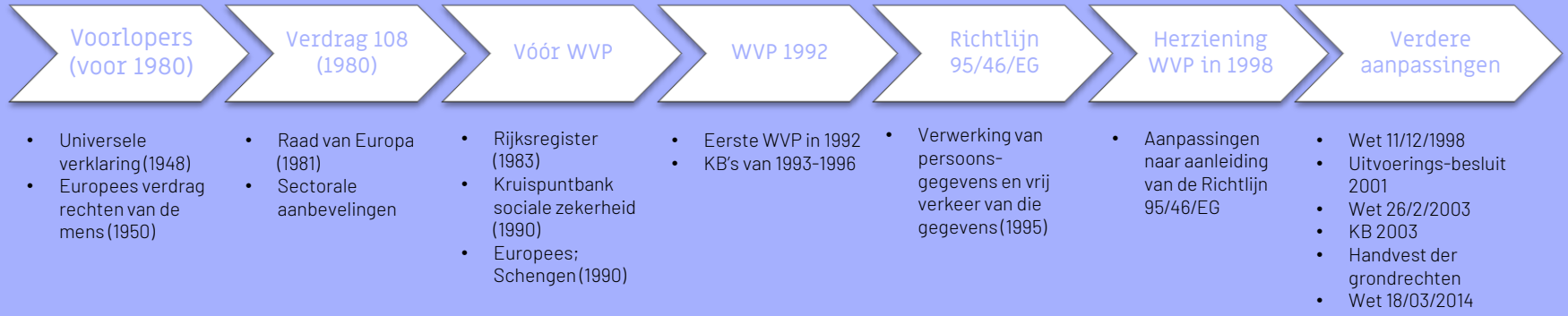


Here’s….
GDPR.



Revolutie of Evolutie?

Nieuwe tijden nieuwe (privacy)wetten



Met de beste bedoelingen

PRIVACY

Zwarte doos onder bureau: bankpersoneel Barclays schrikt van "Big Brother-achtig toezicht"

19-08-17, 19.48u - Peter de Waard

©REUTERS 1

Personeel van de Britse grootbank Barclays is opgeschrikt door onder de bureaus aangebrachte zwarte dozen. Bij navraag bleek het te gaan om bewegings- en warmtesensoren waarmee het bedrijf kan vaststellen wie al dan niet aan zijn bureau zit, en hoe lang. Het gaat om het systeem OccupEye dat in Groot-Brittannië zelf is ontwikkeld. Barclays zegt met de inspraakorganen en de bonden over het aanbrengen van deze apparatuur te hebben

… of met andere redenen?

RECLAMEBORDEN BESPIEDEN SHOPPERS

De Backer vraagt onderzoek naar reclameborden met camera

06/09/2017 om 08:23 | Bron: BELGA

Foto: Peter Hilz

Multinational JCDecaux heeft in Belgische winkelcentra reclameborden geplaatst met een camera. Zo probeert het bedrijf interessante info voor adverteerders te verzamelen, maar volgens privacyexperts is het onwettig. Dat schrijven De Morgen en Het Laatste Nieuws woensdag. Staatssecretaris voor Privacy Philippe De

Bewakingscamera's volgen ons koopgedrag

Beveiligingscamera's in winkels zijn er niet alleen meer om winkeldiefstal te voorkomen, ze worden tegenwoordig veel breder ingezet.

Met slimme software kunnen ze namelijk alles analyseren wat de klant in de winkel doet.

Big Brother

Als bijvoorbeeld een schap veel bezocht wordt en een ander niet, dan kan de winkelier de inrichting aanpassen. Ook kan met de camera's het koopgedrag worden bekeken. Kortom, Big Brother in de winkel.

In uw huiskamer…

… of in de speelkamer?

DeMorgen. Cult. Muziek, film, tv, expo Zine. Interview, foto, lifestyle

Cultuur > Technologie

KINDERSITES

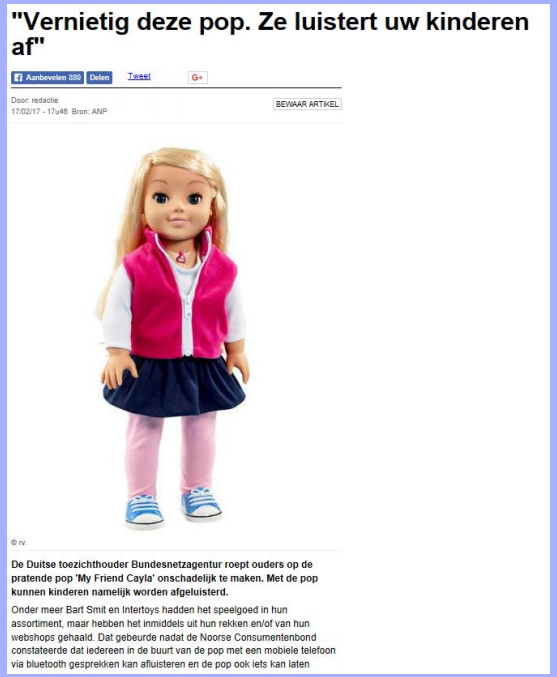
Uw kind wordt getrackt: "Een onwettelijke vorm van informatiegaring"

15-09-16, 06.36u - MAARTEN RABAEY

Maja de Bij, een hyperpopulair Studio 100-figuurtje ©rv

De Privacycommissie waarschuwt kinderwebsites dat ze er op moeten toezien dat surfgedrag en data van minderjarige gebruikers niet worden verhandeld. Uit onderzoek van 72 kinderwebsites (+), waaronder Studio 100, blijkt dat zij door zeker 179 datamakelaars werden gevolgd. "Een onwettelijke vorm van informatiegaring", zegt voorzitter Willem Debeuckelaere.

104 SHARES



"Vernietig deze pop. Ze luistert uw kinderen af"

Aanbevelen 889 Delen Tweet G+

Door: redactie
17/02/17 - 17u46 Bron: ANP

BEWAAR ARTIKEL

© rv.

De Duitse toezichthouder Bundesnetzagentur roept ouders op de pratende pop 'My Friend Cayla' onschadelijk te maken. Met de pop kunnen kinderen namelijk worden afgeluisterd.

Onder meer Bart Smit en Intertoys hadden het speelgoed in hun assortiment, maar hebben het inmiddels uit hun rekken en/of van hun webshops gehaald. Dat gebeurde nadat de Noorse Consumentenbond constateerde dat iedereen in de buurt van de pop met een mobiele telefoon via bluetooth gesprekken kan afluisteren en de pop ook iets kan laten

ING wint Customer Data Award

Elsbeth Eilander, redactie | 8 november 2013, 8:01

ING heeft gistermiddag de Customer Data Award in ontvangst genomen.

De uitreiking vond plaats tijdens het DDMA congres ‘Data en Dialoog in de praktijk’. ING

Het goede voorbeeld geven...

De Standaard Meest recent Binnenland Buitenland Opinie Biz Cultuur Sport Life&Style Beroemd&Bizar Wetenschap Meer ▼

Abonneer u

ING België wil betaalgegevens van klanten gebruiken

13/02/2015 om 15:51 door Wle | Bron: DS/BELGA

G+ Tweet Delen Mail Print

14°C 34

Foto: IMAGEGLOBE

ING België wil de schat aan klanteninformatie waarover ze beschikt, gericht gaan gebruiken. Bedoeling is om 'de klant een goede service aan te bieden'. Van doorverkopen van de data zou geen sprake zijn.

HOME
BIZNIEUWS
ECONOMIE
BEDRIJVEN
MARKETING & MEDIA
CONSUMENT
BEURS
MOBILIA
BELEGGEN
MIJN GELD
EXPERTS
BEREKEN ZELF

Stel ons uw geldvragen

De economieredactie beantwoordt elke lezersvraag over geldzaken.

Stuur ons uw vraag ›
Lees de geldvragen ›

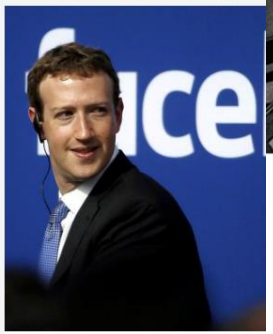
NU IN DS AVOND

… maar wel blijven volhouden!

Misbruik van gegevens

Facebook-privacyschandaal deint uit: "Cambridge Analytica is maar topje van ijsberg"

06-04-18, 06.00u - Freek Evers en Remy Amkre



Marketeers konden op Facebook eenvoudig, en zonde terugvinden. © REUTERS

Facebook verkeert, na de onthullinge Cambridge Analytica, in zwaar weer. die uit de biecht klapt, is er nog veel van woorden kon je heel gericht naa

1 SHARES Facebook Twitter LinkedIn

Adtrackers en zogenaamde **AdOps** zijn al jaren het wilde westen op het internet. Deze bedrijven zorgden voor **super targeted ads** (waarbij op een fractie van een seconde de juiste advertentie voor jouw online profiel wordt gekozen via **Real Time bidding** of ook wel RTB).

Afgelopen week is er nu veel heisa over, daar er nu een studie is verschenen hoe enkele van die trackingscripts een lang gekende browserbug gebruiken om jouw profielgegevens uit websites te slurpen.

HOE WERKT HET?

1. **Jij maakt een profiel** aan op een krantenwebsite of ecommerce webshop
2. Je geeft de **paswoordmanager van je browser** de toestemming om username, paswoord, invulvelden op te slaan.
3. Wanneer je nu op de website surft en een (externe) tracker staat op de website, dan kan die tracker via Javascript **een verborgen formulier plaatsen**, waarna je browser dit **automatisch gaat invullen** (je hebt die daar dan ook toestemming voor gegeven).
4. Met alle **onderschepte gegevens** kan de tracker je onlineprofiel verder aanscherpen (en monetizen in het geval van bijvoorbeeld onAudience)

DATALEK+

uc genaamd 'scraping'

Eigen berichtgeving

hine ter wereld is doorgeslagen", en dat
seffen volgens digitaal marketeer Herman
verleden alle mogelijke marketingtrucs om
verkopen en kent Facebook op zijn

ondertussen boswachter is geworden, is
Maes, digitaal marketeer bij het agentschap
belangrijk dat iedereen beseft dat wat nu
er Facebook en Cambridge Analytica geen
, het is het topje van de ijsberg."

0 SHAR

Datalekken

/Umc-ziekenhuis meldt datalek door gestolen usb-stick met
patiëntgegevens

Het Amsterdamse VU medisch centrum heeft bekendgemaakt dat eerder deze maand een usb-stick is gestolen met daarop patiëntgegevens. Het gaat om gegevens van in totaal bijna 2000 personen. De gegevens bevatten onder andere informatie over 'bij het ziekenhuis uitgevoerde handelingen'.

In een mededeling op zijn website schrijft het ziekenhuis dat het gaat om identificerende gegevens en laboratoriumdata. Deze waren door een verkeerde instelling van apparatuur tijdens onderhoud op de usb-drive van een medewerker van Roche Diagnostics terechtgekomen. Dit was niet de bedoeling, aldus het ziekenhuis. De usb-drive is vervolgens van een medewerker van het diagnostiekbedrijf gestolen.

Naar aanleiding van het datalek heeft het VUmc melding gemaakt bij de politie en bij de Autoriteit Persoonsgegevens. Bovendien zijn er met het bedrijf 'verscherpte protocollen' afgesproken om gegevensverlies te voorkomen. De getroffen patiënten hebben volgens het ziekenhuis een brief ontvangen.

Vorig jaar en vorig jaar meldden ziekenhuizen eerder datalekken, in beide gevallen door een gestolen laptop met daarop patiëntgegevens. De Autoriteit Persoonsgegevens maakte in november bekend dat ziekenhuizen in 2016 verantwoordelijk waren voor 304 meldingen van in totaal 4700 datalekken. Sinds januari 2016 is het verplicht om datalekken te melden.

Autoriteit Persoonsgegevens: '12 datalekken gemeld door onderwij

Onderwijsinstellingen hebben sinds 1 januari dit jaar 126 keer een datalek ge
Alex Commandeur, hoofd Toezicht Publieke sector van de Autoriteit Persoon
op de werkconferentie Informatiebeveiliging en Privacy van Kennisnet. "De vr
wanneer je met een datalek te maken krijgt."

Wie zijn de 61.000 Facebook-Belgen?

© afp

61.000 Belgen zijn 'mogelijk' het slachtoffer van het datalek bij Facebook, maakte het bedrijf gisteravond bekend. Wie zijn die 61.000, en hoe kan hun informatie worden misbruikt?

informatie kwijtgeraakt. Het ministerie van Buitenlandse Zaken noemt het verlies 'bijzonder vervelend'.

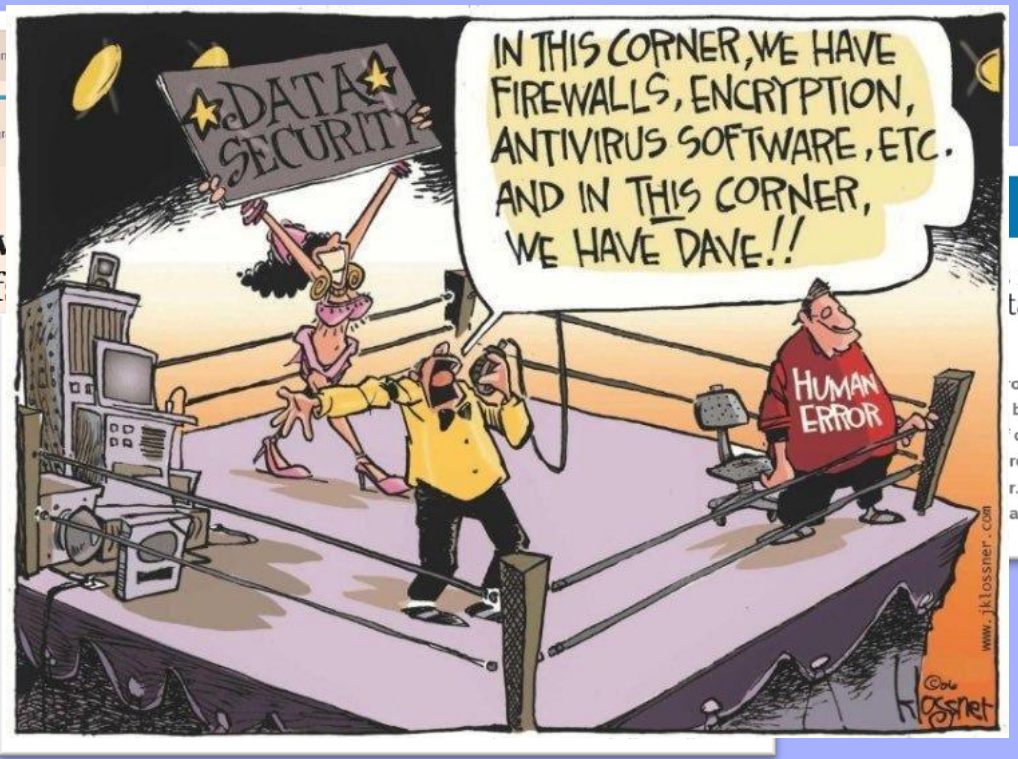
rij omdat

stitie belangrijke
n Brussel heeft
n.

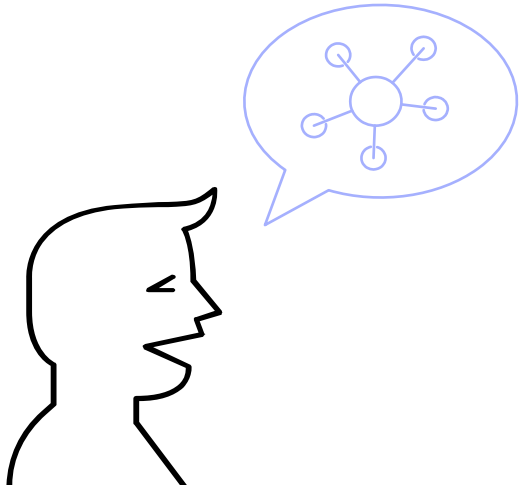
elt gevoelige gegevens van half miljoen patiënten

n geslaagd om de gegevens van een half miljoen
en te bemachtigen. Het gaat om hun
ailadressen en telefoonnummers. Er zijn geen
rs gelekt, maar wel de reden waarom ze
le dokter gingen. De hacker vond een lek in de
en gebruiken om afspraken te regelen via hun

De zwakste schakel



Beter voorkomen dan genezen



Kosten van een datalek

- Forensisch onderzoek
- Communicatie kosten
- Herstelkosten
- Juridische kosten
- Claims van consumenten
- ?Boete van Privacy Commisie?

GDPR is van toepassing op:

IEDEREEN** die **(EU-) PERSOONSGEGEVENS VERWERKT

Wanneer spreken we over persoonsgegevens?

Art. 4 AVG

"Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene");

als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon".

Alle informatie

- ✓ Gegevens
- ✓ Geluid
- ✓ Beeld

Over (betreffende)

- ✓ Betrekking op persoon
- ✓ Rijksregister
- ✓ Locatie
- ✓ Online identificator

Identificatie

- ✓ (In)direct
- ✓ Redelijkerwijs te identificeren

Persoon

- ✓ Enkel levende personen
- ✓ Niet ongeboren
- ✓ Geen rechtspersonen
- ✓ Professionele gegevens = persoonsgegevens

Persoonlijke data

Art. 9,10 AVG

Geen persoonlijke data

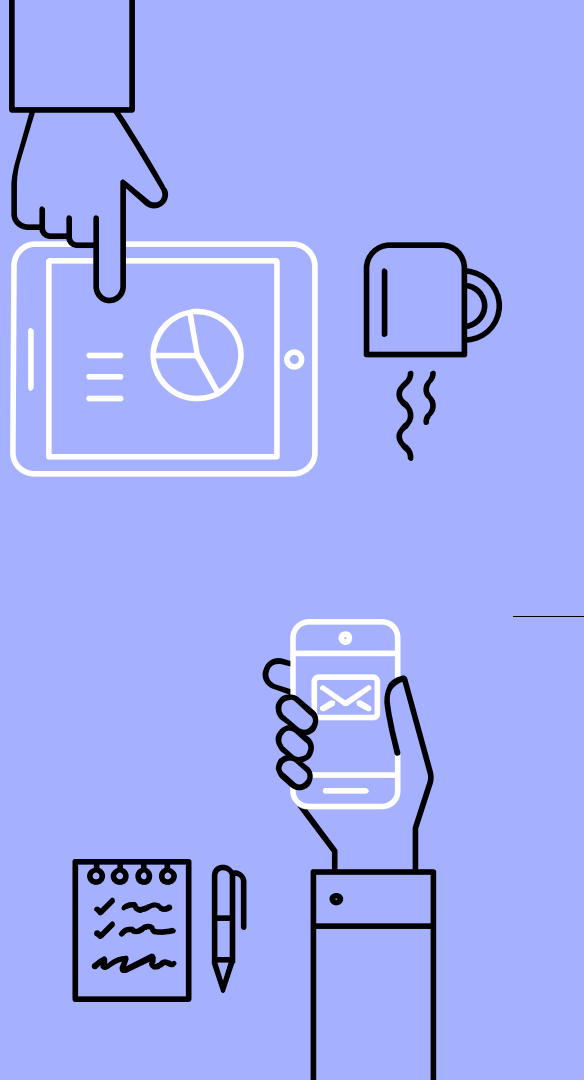
- Bedrijfs-informatie
- Anonieme data
- Geaggregeerde informatie

Persoonlijke data

- Gepseudomiseerde data
- Gevoelige data
- Geëncrypteerde data

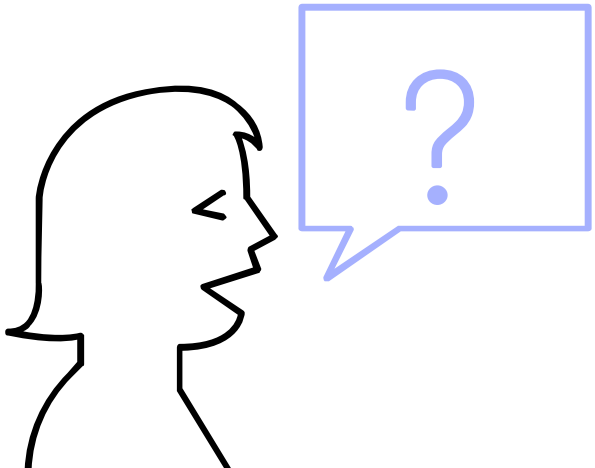
Gevoelige data

- Gegevens over gezondheid
- Ras of etnische afkomst
- Politieke opvattingen
- Lidmaatschap van een vakbond
- Biometrische gegevens
- Strafrechtelijke veroordelingen
- Genetische data



Persoonlijke data

Art. 9 AVG



Mag gevoelige data verwerkt worden?

Principieel verbod op verwerking, met 10 uitzonderingen:

- Betrokkene heeft toestemming gegeven.
- Noodzakelijk i.f.v. wetgeving op het gebied van werkgelegenheid, sociale zekerheid en bescherming.
- Noodzakelijk o.w.v. vitale belangen.
- Ledenbeheer door een stichting met een politiek, filosofisch, religieus of vakbondsdoel.
- Door betrokkene openbaar gemaakt zijn
- Gezondheidszorg binnen de onderneming
- Algemeen belang volksgezondheid

Persoonlijke data

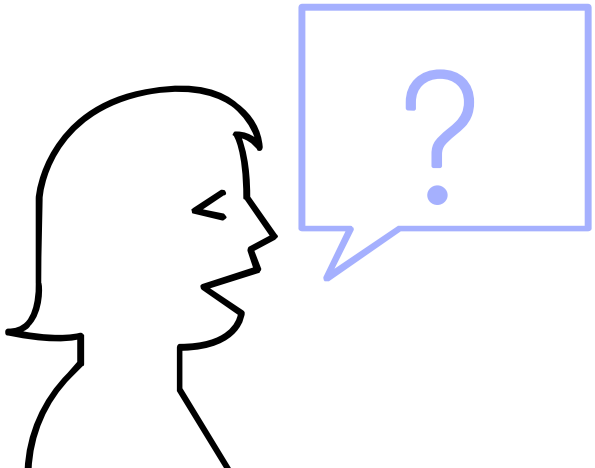
Art. 8 AVG

Vanaf welke leeftijd kunnen persoonsgegevens verwerkt worden?

- GDPR stelt vanaf 16 jaar.
- Bij personen <16 jaar, is ouderlijke toestemming vereist.

Hoe?

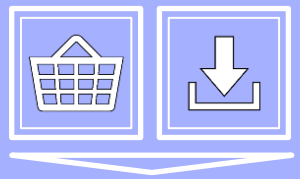
- De voor de verwerking verantwoordelijke stelt alles in het werk om in dergelijke gevallen na te gaan of de houder van de ouderlijke verantwoordelijkheid voor het kind toestemming verleent of machtigt, rekening houdend met de beschikbare technologie.
- De lidstaten kunnen bij wet voor deze doeleinden een lagere leeftijd voorschrijven, mits deze lagere leeftijd niet jonger is dan 13 jaar.
- Voor sociale media binnen België: advies 13 jaar.
- https://www.kinderrechtencommissariaat.be/sites/default/files/bestanden/2015_2016_09_advies_eu_dataprotectie_sociale_media_vanaf_13jaar_def.pdf



Verwerken van persoonsgegevens

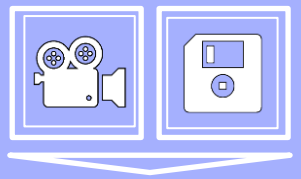
Art. 4 AVG

Verzamelen



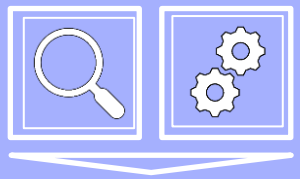
- ✓ Verzamelen
- ✓ Opnemen
- ✓ Afleiden

Opslaan



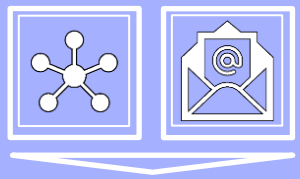
- ✓ Opslaan
- ✓ Structureren
- ✓ Bewaren
- ✓ Organiseren

Gebruiken



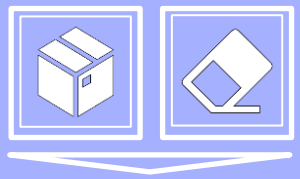
- ✓ Raadplegen
- ✓ Consulteren
- ✓ Bekijken
- ✓ Updaten
- ✓ Wijzigen
- ✓ Combineren
- ✓ Linken
- ✓ Actualiseren

Transfereren



- ✓ Delen
- ✓ Mailen
- ✓ Verzenden

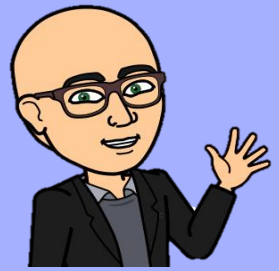
Archiveren



- ✓ Wissen
- ✓ Verwijderen
- ✓ Archiveren

Welke rollen zijn van toepassing?

bol.com



Welke rollen zijn van toepassing?

Betrokkene (of data subject)

Een geïdentificeerde of identificeerbare persoon.
Natuurlijk persoon (ook zakelijke contactgegevens)

Verwerkingsverantwoordelijke (of controller)

Een natuurlijk- of rechtspersoon, overheidsinstantie, agentschap of een ander orgaan die/dat, alleen of samen met anderen, **het doel en de middelen** voor de verwerking van persoonsgegevens **vaststelt.**

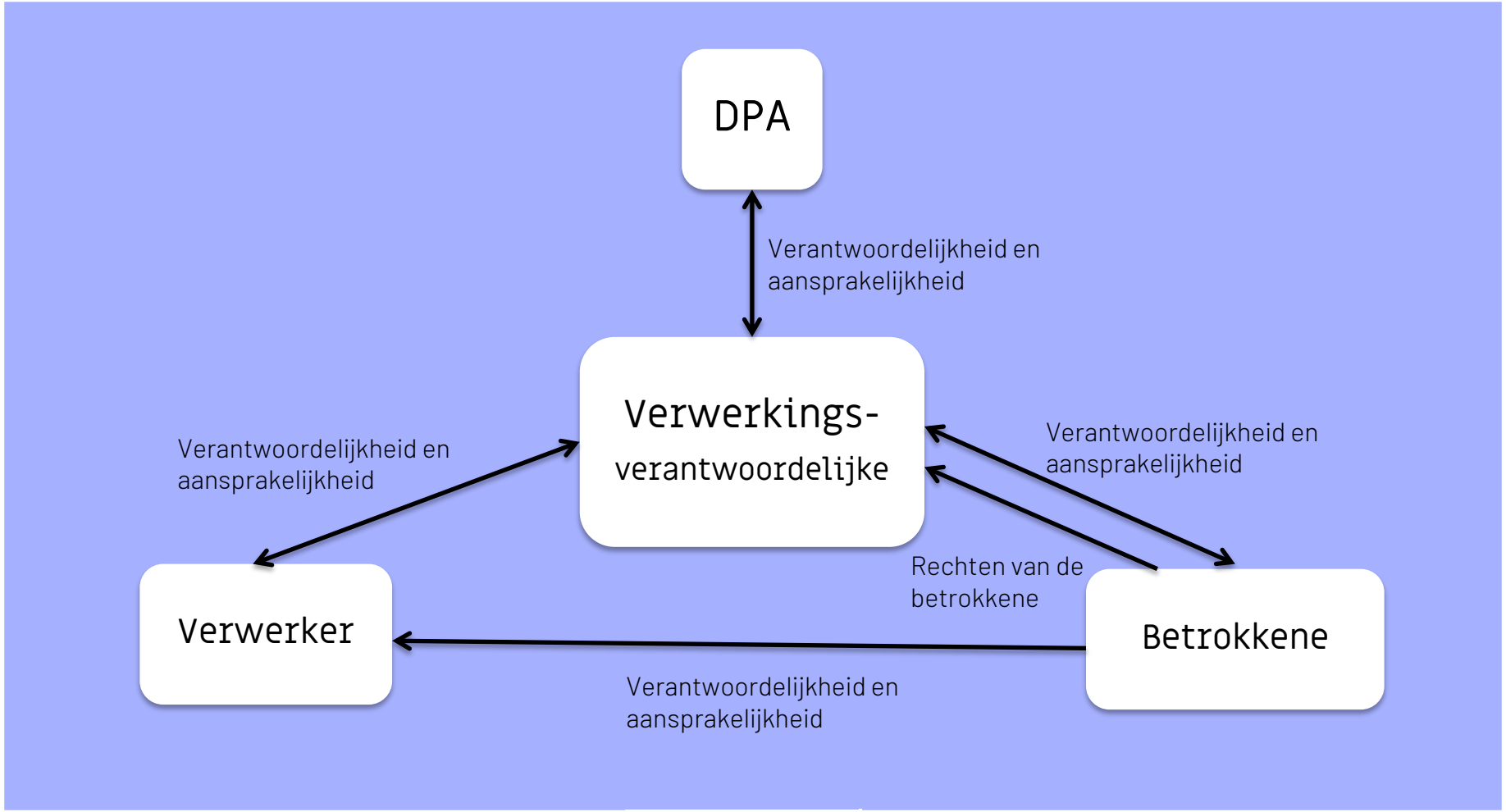
bol.com

Verwerker (of processor)

Een natuurlijk- of rechtspersoon, overheidsinstantie, agentschap of een ander orgaan die/dat **ten behoeve van** de verwerkingsverantwoordelijke (of controller) persoonsgegevens verwerkt

Gegevensbeschermingsautoriteit (of Data Protection Authority - DPA)

Een onafhankelijk ingestelde overheidsinstantie die zich richt op supervisie, compliance, klachten, accountability, boetes, … In België CBPL (of Privacycommissie).


DPA
Verantwoordelijkheid en aansprakelijkheid
Verwerkings-verantwoordelijke
Verantwoordelijkheid en aansprakelijkheid
Verantwoordelijkheid en aansprakelijkheid
Rechten van de betrokkene
Verwerker
Betrokkene
Verantwoordelijkheid en aansprakelijkheid

Voor welke onderneming is de GDPR van toepassing?

- De verwerkingsverantwoordelijke of verwerker een vestiging binnen de EU heeft.

Indien er geen vestiging is binnen de EU maar wel

- **Diensten of goederen** aangeboden worden **aan betrokkenen binnen EU**. (al dan niet betalend)
- Betrokkenen **gevolgd worden** voor zover gedrag plaats vindt **binnen de EU**. (bv track & tracing)

Rechten van de betrokkene

Recht op informatie

Recht op inzage

Recht wissen van gegevens

Recht op data overdraagbaarheid

...

GDPR Principes

Rechtmatigheid van de verwerking

Doelbinding

Minimale gegevensverwerking

Juistheid

Opslagbeperking

Integriteit & vertrouwelijkheid

Technische maartregelen

Security

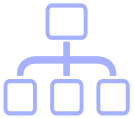
Encryptie

Authenticatie

Authorisatie

Anonimisatie

Pseudonimisatie



Organisatorische maatregelen

Interne privacy policies

Interne security policies

Opslag van gegevens

Bewustwordingssessies

Verantwoordelijk heden

Verwerkingsregister

Melding datalekken

Aanstellen DPO (indien vereist)

Privacy by default/design

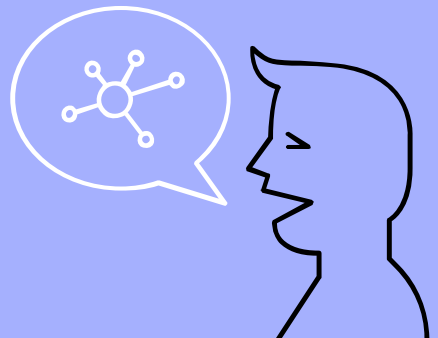
Third party

Data Transfer buiten EU

Verwerkerscontract met verwerkers

Rechten van de betrokkene

Basis	Eerste optie: actie	Tweede optie: actie	Actie na inzicht	Specifiek recht tijdens inzage
Recht op informatie	Recht om toestemming in te trekken	Recht op inzage/toegang (of kopie)	Recht van verbetering	Recht op beperking van verwerking
Recht op transparantie	Recht niet te worden onderworpen aan profilering	Recht op overdraagbaarheid	Recht op (uit)wissing	
	Recht op bezwaar		Recht op vergetelheid (of ontlinken)	



Waarmee moeten we rekening houden?

- ✓ Betrokkene moet antwoord krijgen binnen één maand
  (kan verlengd worden afhankelijk van de complexiteit van de verzoeken of van het aantal)
- ✓ Gratis
- ✓ Duidelijke taal
- ✓ Confidentieel: betrokkene moet mogelijk identiteit bewijzen

Basisprincipes GDPR

Rechtmatigheid van verwerking

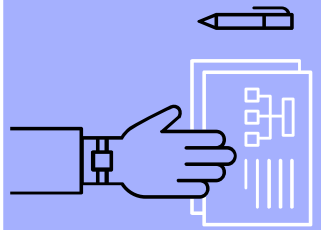
Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.

Minimale gegevensverwerking

Proportionaliteitsbeginsel: persoonsgegevens dienen toereikend en ter zake dienend te zijn en beperkt te blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

Juistheid

Persoonsgegevens moeten juist zijn en, zo nodig, worden geactualiseerd.
Alle maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.



Doelgericht

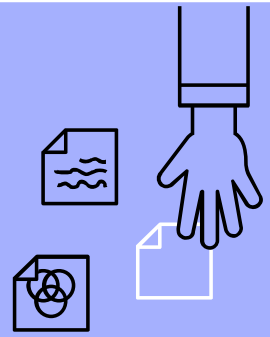
Finaliteitbeginsel: persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Persoonsgegevens mogen (vervolgens) niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.

Opslagbeperking

Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkene niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt, noodzakelijk is.

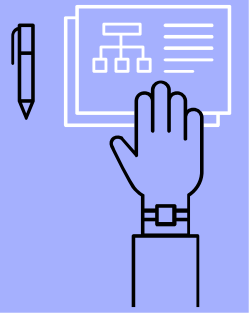
Transparantie

Persoonsgegevens moeten verwerkt worden in een transparantie manier in relatie met de betrokkene.



Integriteit en vertrouwelijkheid

Persoonsgegevens moeten, door het nemen van passende technische of organisatorische maatregelen, op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.



Transparant, eerlijk en rechtmatige verwerking

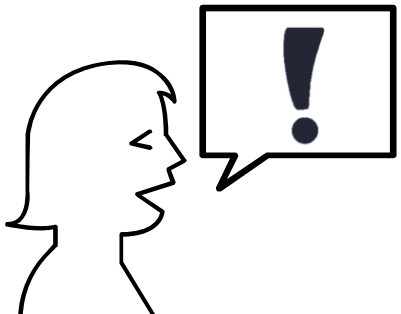
DUIDELIJKE omschrijving wat u met de gegevens gaat doen, waarom, wie, waar en voor hoelang.

Bv. bezoekers registratie.
Voor de veiligheid wil u weten wie er op uw bedrijf aanwezig is, wat de reden van bezoek is en bij wie hij is. U houdt dit enkel bij in het register en de gegevens worden dagelijks gewist.

Rechtmatige verwerking

Toelaatbaarheidsgronden

- Uitvoering overeenkomst
  - *vb. klant – leverancier relatie*
- Wettelijke verplichting
  - *Vb bijhouden van boekhoudkundige gegevens, personeelsdata, witwasbestrijding,…*
  - *https://www.merak.be/be-nl/kenniscenter/legal-bewaartermijnen*
- Vitaal belang
  - *Belang moet levensbedreigend zijn, geen andere grondslagen mogelijk*
  - *Zeer restrictief gebruiken!*
- Algemeen belang
  - *Vooral voor ordediensten en openbare besturen*
- Gerechtvaardigd belang
  - *Vb. vrijheid van ondernemen, recht op informatie, …*
  - *Mag geen nadeel voor de betrokkene vormen!*
- Toestemming



Rechtmatige verwerking

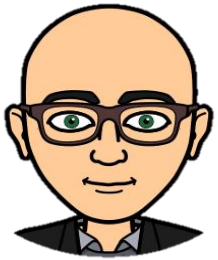
Expliciete toestemming (consent)

Een toestemming moet:

- Vrij en specifiek zijn
- Berusten op informatie
- Door een ondubbelzinnige actieve handeling of verklaring

Verenigbaar met het doel van de verwerking

Doelbinding en onverenigbaarheids-beoordeling

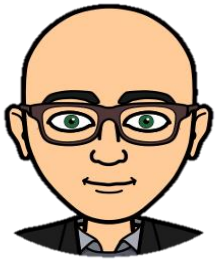


Doel:

- ✓ Op de hoogte houden van promoties (direct marketing)
- ✓ Contacteren voor afspraak in showroom

Verenigbaar met het doel van de verwerking

Doelbinding



! Doorgeven/verkopen gegevens aan derden (leveranciers, financiële instellingen, ...)

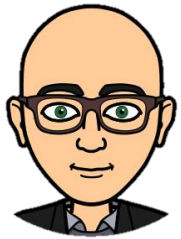
Minimale gegevensverwerking

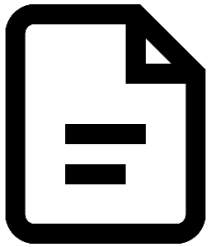
LESS IS MORE

Nice to know vs Need to know

Vb1. Als het volstaat om de leeftijd (jaar van geboorte) te weten vraag dan niet naar geboortedatum.
Vb2. Inlezen van volledige paspoortgegevens voor garantie?

Minimale gegevensverwerking





- ✓ Naam, adres, telefoonnummer, emailadres
- ✓ Regio
- ✓ Periode beslissing

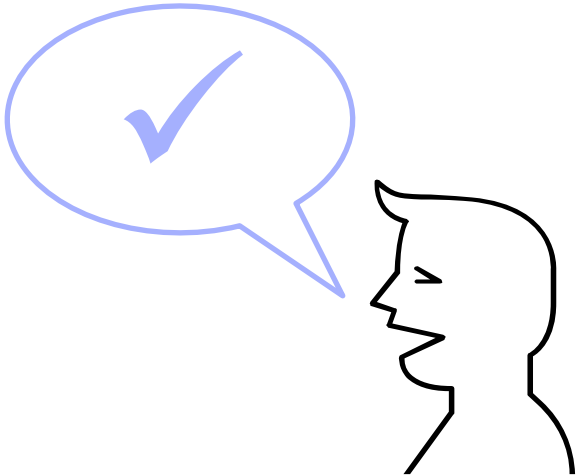
- ! Geboortedatum
- ! Burgerlijke stand
- ! Bewijs eigendom, lening, ...

Juistheid

Vb1. Bij direct marketing

- ✓ *"delivery returns" en "bounces" na een mailing adressen wissen of corrigeren*
- ✓ *Unsubscribe – wissen uit ALLE databases*

Vb2. Adresgegevens van een klant wijzigen na verhuis & oud adres wissen.



Opslagbeperking

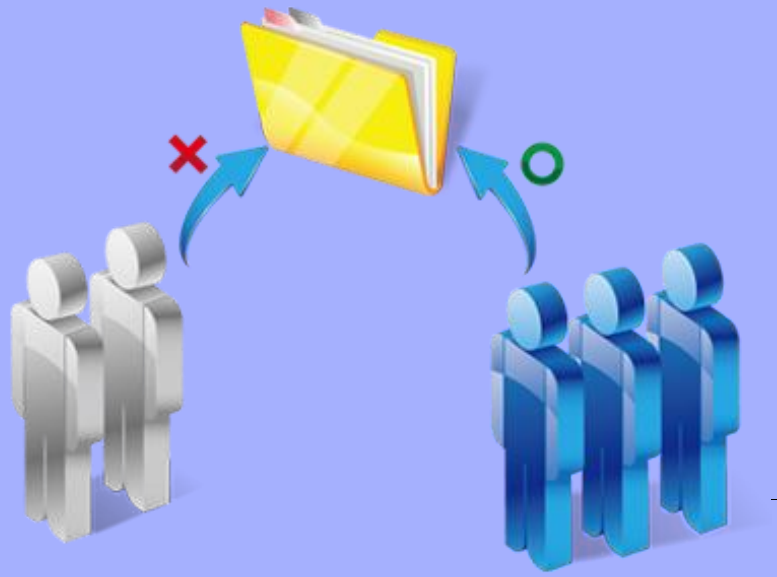
Sla gegevens niet onnodig lang op. Als er geen wettelijke bewaartermijn bestaat stel er dan zelf een op. Voorzie minstens criteria.

Vb.

1. *Definieer hoelang een klant "klant" blijft.*
2. *Wis persoonsgegevens.*
3. *Uitzondering bv. wettelijke bewaartermijn boekhoudkundige gegevens*

Integer en vertrouwelijk

Zorg dat iedere medewerker de juiste rechten/toegangen heeft en weet hoe hij met de gegevens dient om te gaan.

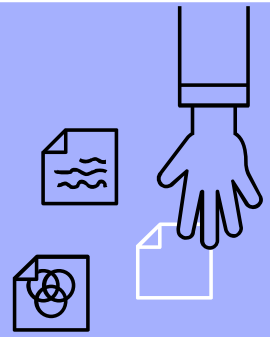


Vb. Klantgegevens:

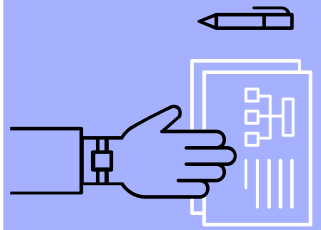
1. *Sales kan aanmaken & corrigeren*
2. *Facturatie kan corrigeren*
3. *Marketing kan consulteren*
4. *Interne onderhoudsploeg heeft geen toegang.*

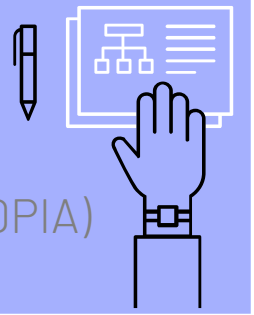
Welke zijn de verantwoordelijkheden voor een organisatie?

Verantwoordelijkheden



- ✓ Verwerkingsregister
- ✓ Verwerkerscontract
- ✓ Melden van gegevenslekken
- ✓ Dataprotection by default/by design
- ✓ Data protection officer (DPO)
- ✓ Risico-analyse bij nieuwe technologieën of processen (DPIA)





Verwerkings-register

- Is een basisdocument ifv nakomen van de GDPR.
- Bevat ALLE data verwerkingsactiviteiten die uitgevoerd worden.
- Zowel van toepassing bij verantwoordelijke als verwerker.
- Is geen statisch document.
- Moet niet gedeeld worden met de DPA, maar DPA kan het wel opvragen.

Privacy commissie link:
https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten

Wordt er persoonlijke data verwerkt ten behoeve van u?

Verwerkers-contract

Een verwerkerscontract moet opgesteld worden met elke verwerker

De verwerkingsverantwoordelijke doet uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de veristen van de GDPR voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

- ✓ Contract bevat verplichtingen verwerkingsverantwoordelijke - verwerker
- ✓ De persoonsgegevens uitsluitend verwerkt worden o.b.v. schriftelijke instructies van de verwerkingsverantwoordelijke
- ✓ Werknemers van de verwerker zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen d.m.v. het tekenen van een contract
- ✓ De verwerker neemt passende technische en organisatorische maatregelen m.b.t. beveiligingsniveau
- ✓ De verwerker neemt geen andere verwerker in dienst zonder voorafgaande toestemming van de verwerkingsverantwoordelijke …
- ✓ Bijstand te verlenen wanneer een betrokkene één of meerdere van zijn rechten uitoefent
- ✓ …

Melden van gegevenslekken

Data Breach Risk Assesment

Online:
http://www.breachlevelindex.com/data-breach-risk-assessment-calculator

Manueel:
SE = DPC x EI + CB
(Severity = Data Processing Context x Ease of Identification + Circumstances Breach)
https://www.enisa.europa.eu/publications/dbn-severity

Melden van gegevenslekken

Wie?	Aan?	Wanneer?	Uitzonderingen
Controller	DPA	Binnen 72u	Als het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van de natuurlijke personen.
	Data subject	Onmiddellijk	Als de controller passende (technische en organisatorische) maatregelen heeft genomen die gegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling. **Als controller achteraf maatregelen heeft genomen zodat hoge risico voor rechten en vrijheden van de betrokkenen zich waarschijnlijk niet meer zal voordoen.** Als de mededeling onevenredige inspanningen vergt. Voorstel: openbare mededeling.
Processor	Verantwoordelijke	Onmiddellijk	

Wordt er data verwerkt buiten de EU?

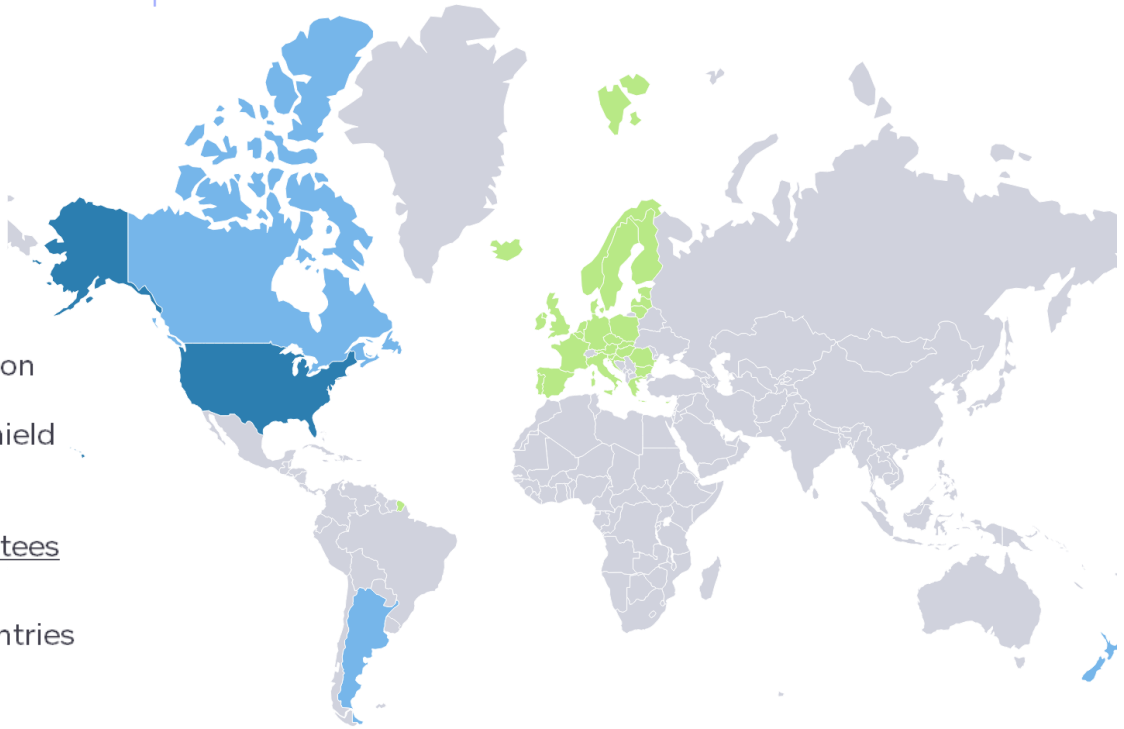
Elke verwerkingsverantwoordelijke moet weten wie zijn data verwerkt en moet deze verwerkers monitoren naar GDPR compliance toe.

Allowed

- Transfer to EEA countries
- Transfer to countries with adequate level of protection
- Transfer EU-US Privacy Shield companies

Not Allowed without additional guarantees

- Transfers to all other countries



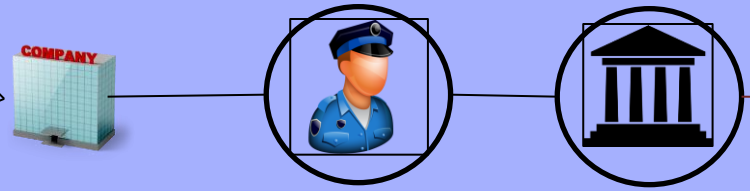
Data Protection Officer (DPO)

Een DPO:

- ✓ Rapporteert aan CEO of management team (die verantwoordelijk is/zijn).
- ✓ Wordt aangewezen op basis van professionele kwaliteiten en deskundigheid.
- ✓ Moet onafhankelijk zijn.
- ✓ Is een rol en niet een persoon.
- ✓ Heeft geheimhoudingsplicht.

Awareness
Informeren
Adviseren
Monitoren
Onderwijzen van werknemers
Auditeren
Rapporteren

Verwerkingsregister
DPIA
Roadmap
Policies



verwerkingsverantwoordelijke
verwerker

Contactpersoon DPA
Informeren ifv data lekken
Samenwerking met DPA

Data Protection Officer

- Vertaald in het Nederlands: Functionaris voor gegevensbescherming
- DPO toewijzen in geval van (bij verwerkingsverantwoordelijke en verwerker)

  Als verwerking wordt uitgevoerd **door overheidsintantie** of-orgaan. (Publieke sector)

  (of)

  Hoofzakelijk belast (=kerntaak) met verwerking die vanwege aard, omvang en/of doeleinden **regelmatig en stelselmatige observatie op grote schaal vereisen**.

  (of)

  Hoofzakelijk belast (=kerntaak) met verwerkingen **op grote schaal van bijzondere categorieën van persoonsgegevens**k

Risico-analyse bij nieuwe technologieën of processen (DPIA)

Gegevensbeschermingseffectenbeoordeling

80 punten

DPIA

- Is een proces dat helpt bij het inschatten van potentiële risico's m.b.t. betrokkene bij het verwerken van hun persoonlijke data.
- Is verplicht aan te maken bij het in gebruik nemen van nieuwe technologie.
- Moet breed in de onderneming gepositioneerd worden (IT + Project Team + Developers + ...)
- DPO adviseert bij de aanmaak van een DPIA (evalueren, controleren, uitdiepen, ...)

https://whitewire.be/wp-content/uploads/2017/06/20170616_template_DPIA.docx

Dataprotection by default

Standaard de meest privacy-vriendelijke instellingen garanderen.

- ✓ Niet enkel opties (vinkjes) maar ook algemene voorwaarden!
- ✓ Geen opt-out maar (double)opt-in regime

Dataprotection by design

Bluetrace moet stoppen met wifi-tracking van omwonenden in winkelgebieden

De Autoriteit Persoonsgegevens heeft een last onder dwangsom aan het Nederlandse bedrijf Bluetrace opgelegd. Het bedrijf moet stoppen met wifi-tracking van omwonenden van winkelgebieden en moet verzamelde gegevens meteen verwijderen of anonimiseren.

Ook moet het bedrijf personen duidelijk informeren over het feit dat er tracking plaatsvindt via wifi, schrijft de privacytoezichthouder. Bluetrace moet deze maatregelen binnen zes maanden doorvoeren en is als het dat niet doet een dwangsom van vijfduizend euro per week verschuldigd, zolang er geen oplossing is. Het maximumbedrag dat op die manier opgelegd kan worden is 100.000 euro, blijkt uit de bijbehorende brief. De Autoriteit Persoonsgegevens had in 2015 al geconstateerd dat het bedrijf de privacywetgeving overtrad door personen te volgen.

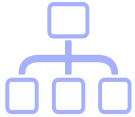
GPS-horloges voor kinderen slecht beveiligd

Els Bellens
Els Bellens is redactrice bij Data News.

18/10/17 om 08:02 - Bijgewerkt om 08:03
Bron: Anp

Ouders die voor hun kind een GPS-horloge kopen in de hoop hen zo veiliger de wereld in de sturen, moeten opletten: de beveiliging van enkele van deze apparaten, met ingebouwde telefoon, laat te wensen over. Dat blijkt uit testen van de Noorse consumentenbond.

Organisatorische maatregelen



- ✓ Awareness sessies
- ✓ Training van werknemers
- ✓ Internal privacy policies
- ✓ Internal security policies
- ✓ Contracten werknemers
- ✓ Monitoring van compliance niveau

Technische maatregelen

- ✓ Security
- ✓ Anonimiseren
- ✓ Authenticatie
- ✓ Autorisatie
- ✓ Encryptie
- ✓ Pseudonimiseren

Welke organisatorische maatregelen?

Boetes ?!?!

Inbreuken op verplichtingen van de onderneming

Tot 10.000.000€ of tot 2% wereldwijde omzet van jaar -1 indien dit cijfer hoger is

Inbreuken op de rechten van de betrokkenen of GDPR principes

Tot 20.000.000€ of tot 4% wereldwijde omzet van jaar -1 indien dit cijfer hoger is

GDPR een opportuniteit?

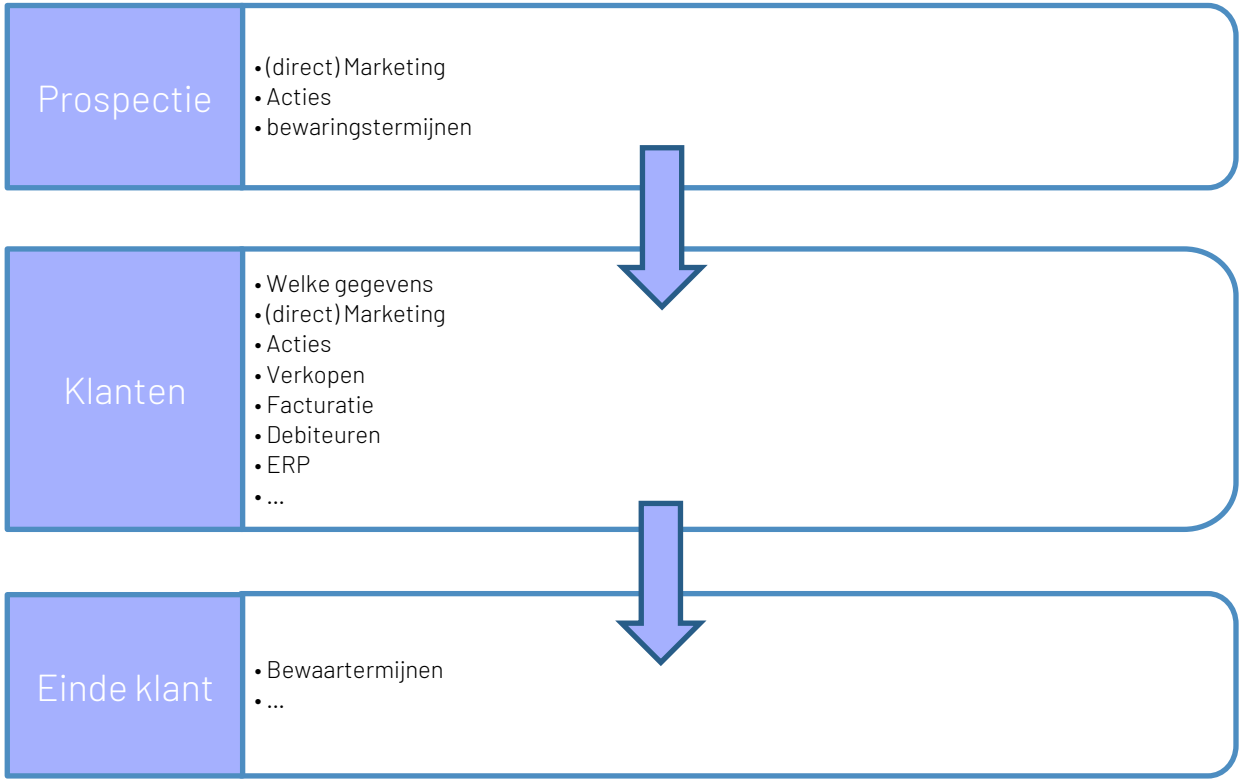
Analyseer en bescherm niet enkel persoonsgegevens maar neem uw gehele bedrijfsgegevens onder de loep!

- Dataverlies
  https://www.merak.be/be-nl/over-merak/pers/4-op-10-belgische-bedrijven-riskeren-dataverlies
- Dubbele (klant)gegevens
- Onvolledige, foute (klant)gegevens
- Decentrale (klant)gegevens
- Oude, overbodige (klant)gegevens
- Ontslag/vertrek van medewerkers

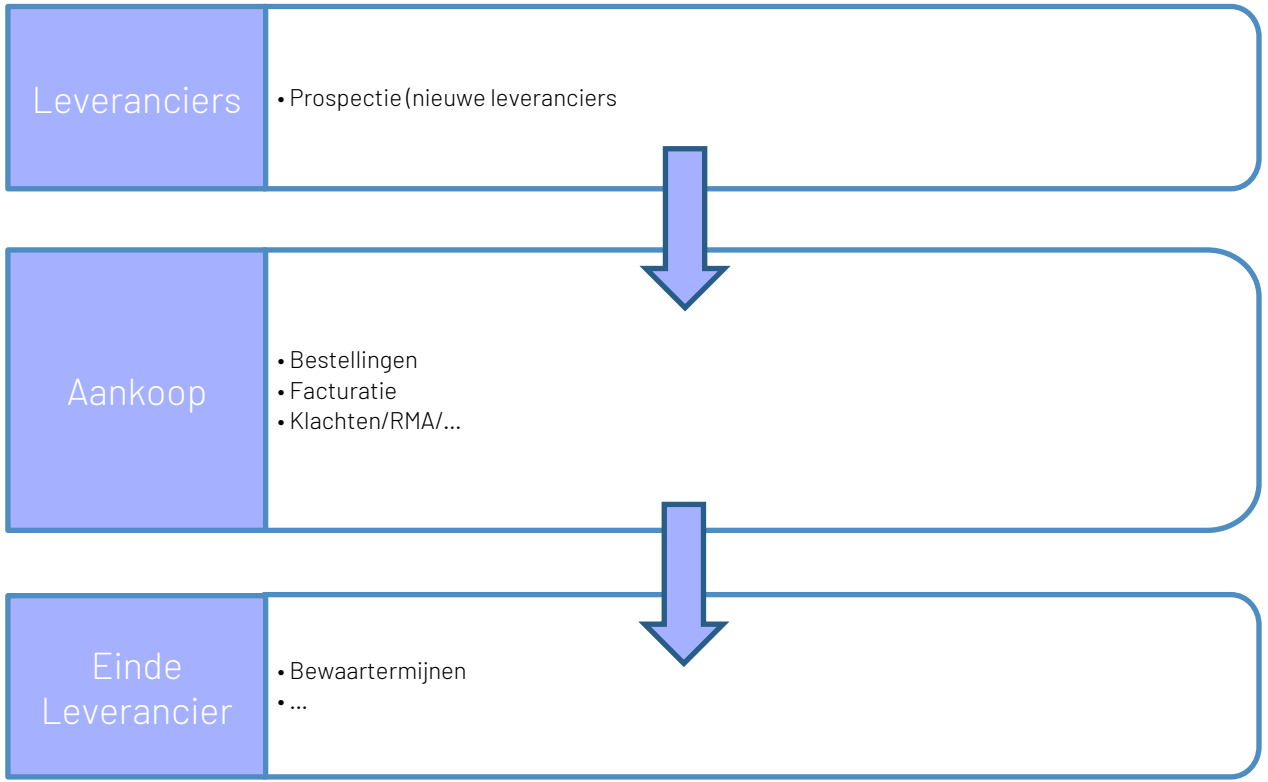

1 2 3 4 5 6 7 8

Voorbeelden van processen

Voorbeeld van processen



Voorbeeld van processen



Voorbeeld van processen

- Sollicitanten
- Personeel
- Interims
- Vakantiejobs
- Stagiairs
- IBO
- …