AVG: Stilte voor de storm?

ICTRECHT

Wie ben ik?

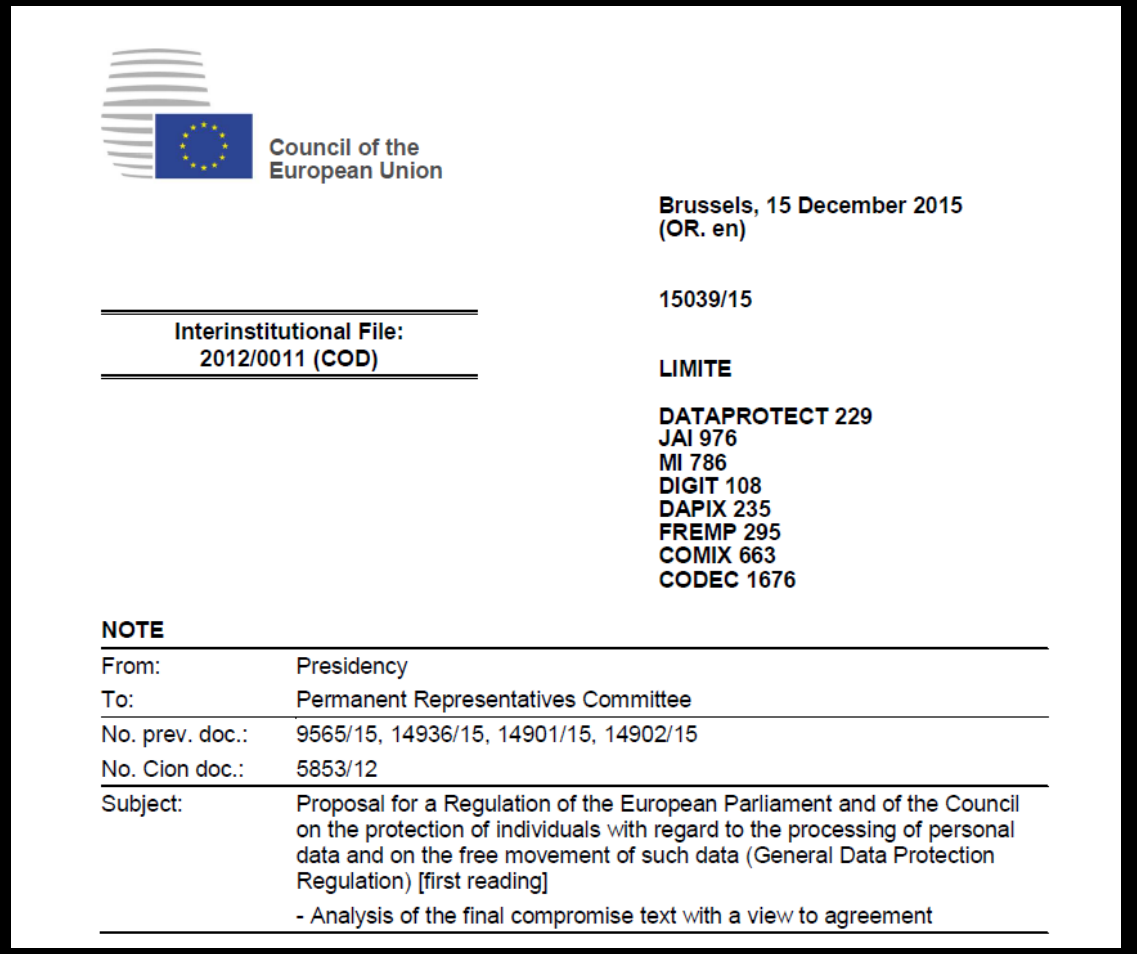
Mr. Dr. Mathieu Paapst

www.ictrecht.nl

Twitter: @paapst

Algemene verordening gegevensbescherming

- Rechtstreekse werking
- In alle lidstaten direct verbindend
- Geen nationale afwijkingen tenzij in verordening toegestaan
- NB: e-Privacy verordening



Council of the European Union

Brussels, 15 December 2015
(OR. en)

15039/15

Interinstitutional File:
2012/0011 (COD)

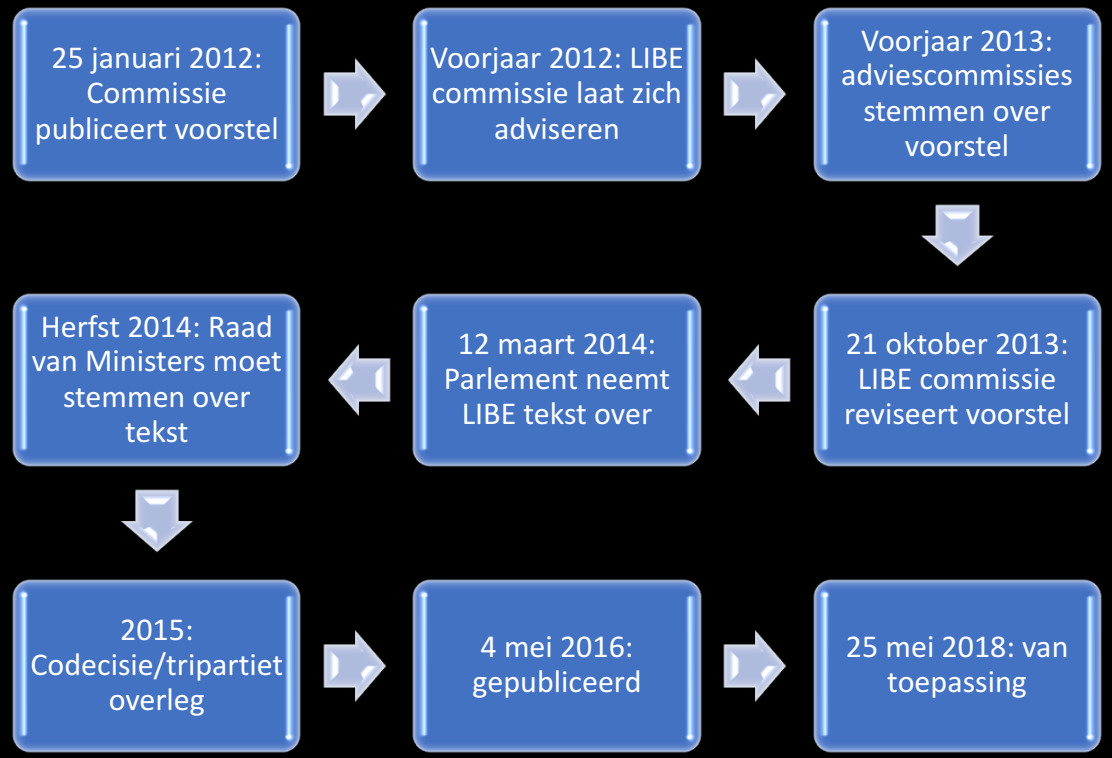
LIMITE

DATAPROTECT 229
JAI 976
MI 786
DIGIT 108
DAPIX 235
FREMP 295
COMIX 663
CODEC 1676

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. prev. doc.:	9565/15, 14936/15, 14901/15, 14902/15
No. Cion doc.:	5853/12
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] - Analysis of the final compromise text with a view to agreement

Tijdlijn Privacyverordening



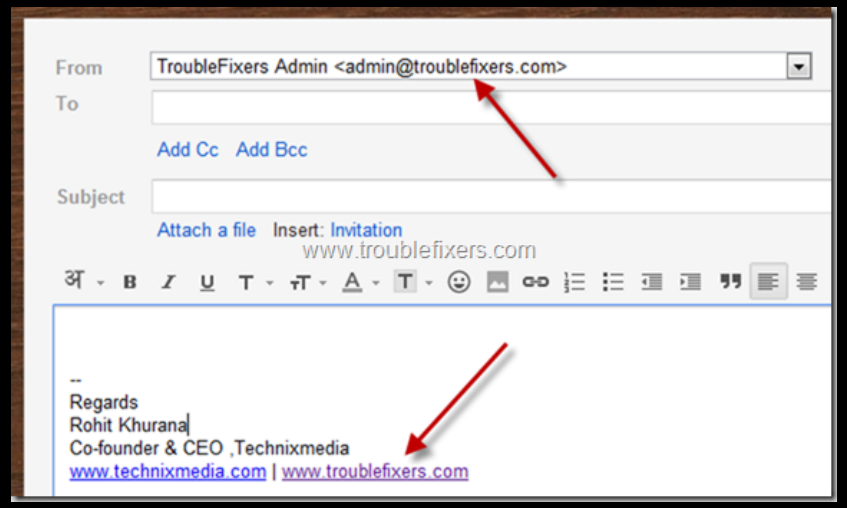
EU Privacy regulations subject to 'unprecedented lobbying'

EU Commissioner Viviane Reding says new regulations on digital privacy are designed 'to stand for 30 years' but were subject to the most aggressive lobbying she has ever witnessed.

"The lobbying from all sides has been fierce – absolutely fierce – I have not seen such a heavy lobbying operation," she said. "But the legislation was on the table on the 25th January as I wanted to have it. So much to the efficiency of lobbying."

EU commissioner Viviane Reding Photo: REUTERS

Persoonsgegevens

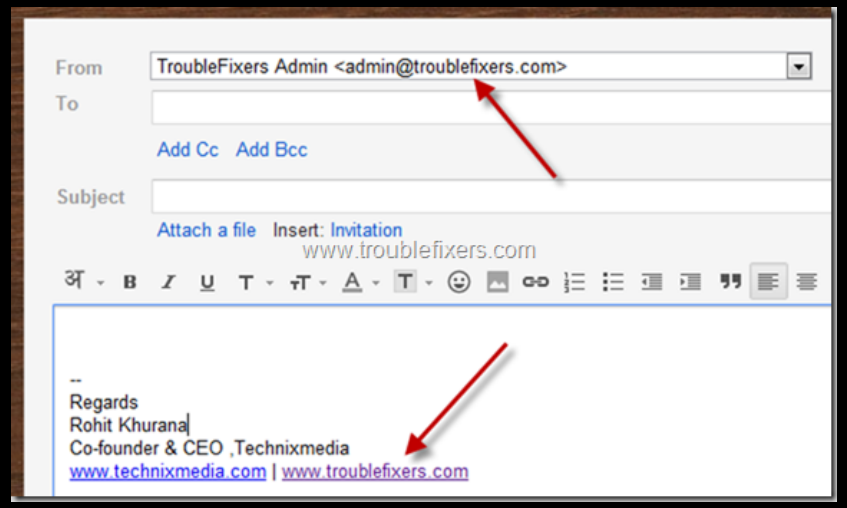


alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon;

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;

Art. 4 (1) AVG

Persoonsgegevens

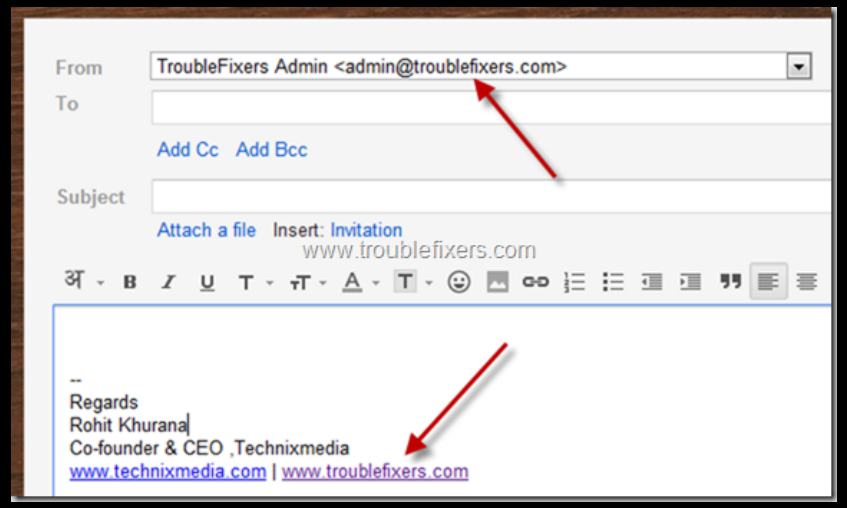


alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon;

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;

Art. 4 (1) AVG

Persoonsgegevens



alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon;

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;

Art. 4 (1) AVG

Grondslagen

- Toestemming
- Uitvoering overeenkomst
- Wettelijke plicht
- Vitale belangen betrokkenen
- Uitvoering overheidstaak
- Dringend eigen belang*

Alleen de gegevens die **noodzakelijk** zijn!

Art. 6 AVG

Toestemming

"elke **vrije**, **specifieke**, **geïnformeerde** en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een **verklaring** of een ondubbelzinnige **actieve handeling** hem betreffende verwerking van persoonsgegevens aanvaardt"

Art. 4 (8) AVG


L
I
F
E
?
?
?
?

Bijzondere persoonsgegevens

…waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid…

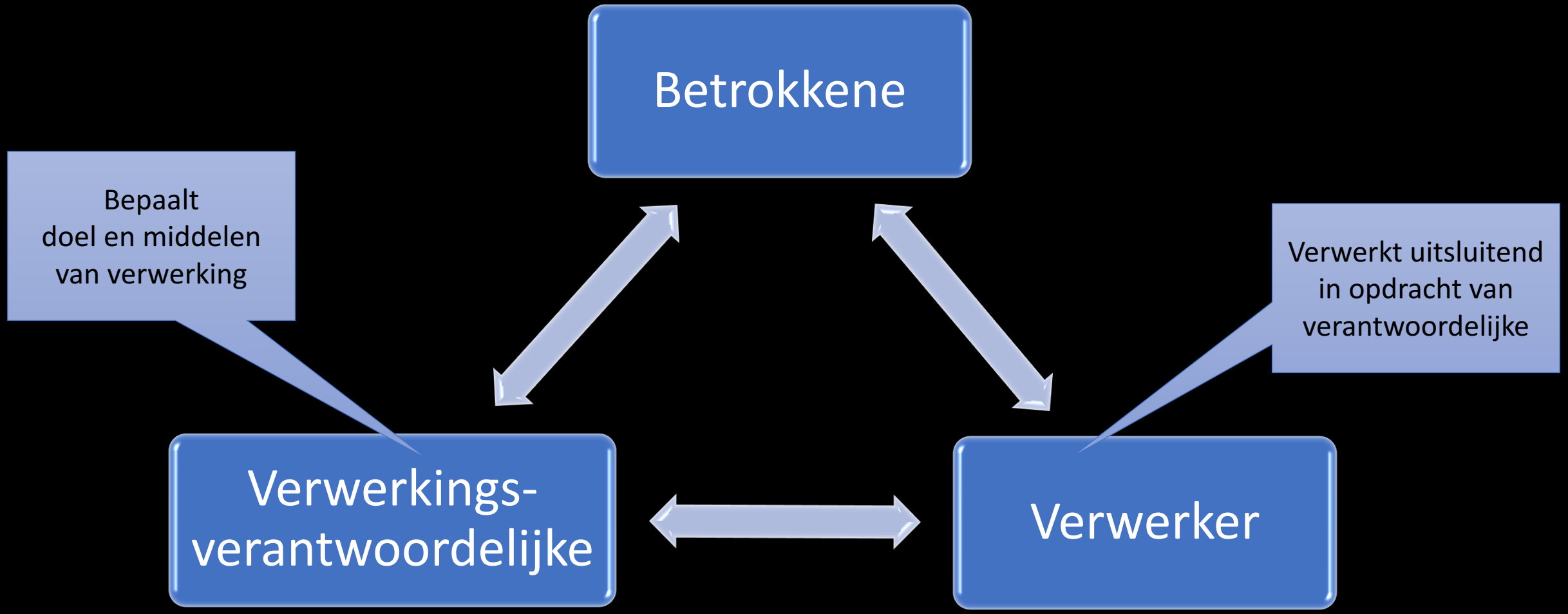
Art. 9 AVG

Grondslagen bijzondere persoonsgegevens

- Expliciete toestemming (tenzij deze niet gegeven mag worden)
- Uitvoering arbeids-, socialezekerheids- en socialebeschermingsrecht (indien apart geregeld in nationale wet)
- Vitaal belang betrokkene
- Regelen lidmaatschap van vakbond, stichting, kerk en dergelijke
- Onmiskenbaar zelf openbaar gemaakt
- Afhandeling juridische claims
- Zwaarwegend algemeen belang
- Gezondheidskwesties/leveren zorg
- Volksgezondheid
- Wetenschappelijk onderzoek, archieven

Art. 9(2) AVG

Terminologie en rollen



Rechten van betrokkenen


Betrokkene
Inzage
Export
Correctie
Klacht
Vertegen-
woordiging
Beroep
Beperking
Schade-
vergoeding
Bezwaar
Vergeten
worden
Geen
profiling

Recht van inzage

- Doelen van verwerking
- Soorten persoonsgegevens
- Ontvangers (ook in derde landen)
- Bewaartermijn
- Recht op uitleg herkomst persoonsgegevens
- Uitleg over de logica bij geautomatiseerde verwerking

Art. 15 AVG

Recht van dataportabiliteit

Is er sprake van:

- Verwerking gebaseerd op ‘toestemming’ of ‘uitvoering overeenkomst’; en
- Verwerking vind geautomatiseerd plaats.

- Verkrijgen van opgeslagen persoonsgegevens
- Elektronische kopie
- In gestructureerde, gangbare en machineleesbare vorm
- Zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke.

Art. 20 AVG

Recht van dataportabiliteit

Is er sprake van:

- Verwerking gebaseerd op ‘toestemming’ of ‘uitvoering overeenkomst’; en
- Verwerking vind geautomatiseerd plaats.

- Verkrijgen van opgeslagen persoonsgegevens
- Elektronische kopie
- In gestructureerde, gangbare en machineleesbare vorm
- Zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke.

Art. 20 AVG

Correctie en rectificatie

- Rectificatie van onjuiste gegevens
- Aanvulling van incomplete gegevens
- Onverwijld

Art. 16 AVG

Uitzondering!!!

- AVG Recht op inzage, rectificatie, dataportabiliteit en bezwaar zijn niet van toepassing indien de gegevens in het Nationaal archief of in de Regionale Historische Centra worden bewaard.
- Betrokkenen krijgt wel het recht om zijn eigen lezing aan het desbetreffende archiefbescheiden toe te voegen (art. 43 lid 3 Uitvoeringswet)

Restrictie

Betrokkene kan restrictie van verwerking eisen als:

- Hij twijfelt aan nauwkeurigheid
- De verwerking onrechtmatig is
- De gegevens niet langer nodig zijn voor verwerking, maar wel voor rechten van betrokkene (juridische claims)
- Hij bezwaar heeft gemaakt tegen grondslag verantwoordelijke

Art. 18 AVG

Recht op gegevenswissing („recht op vergetelheid”)

Recht op gegevenswissing („recht op vergetelheid”)

1. De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:

Art. 17 AVG

Verwijdering en staking gebruik

- Indien gegevens niet meer nodig voor het originele doel
- Indien toestemming ingetrokken en geen andere grond meer
- Indien bezwaar gemaakt
- Indien verwerking onrechtmatig
- Indien wettelijke verplichting

Niet van toepassing als persoonsgegevens nodig zijn voor:

- Vrijheid van meningsuiting (art. 85)
- Uitvoeren van wettelijke plicht
- Openbaar belang
- Archiveringsdoeleinden
- Juridische claims

Art. 17 PV

Verwijdering en staking gebruik

- Indien gegevens niet meer nodig voor het originele doel
- Indien toestemming ingetrokken en geen andere grond meer
- Indien bezwaar gemaakt
- Indien verwerking onrechtmatig
- Indien wettelijke verplichting

Niet van toepassing als persoonsgegevens nodig zijn voor:

- Vrijheid van meningsuiting (art. 85)
- Uitvoeren van wettelijke plicht
- Openbaar belang
- Archiveringsdoeleinden
- Juridische claims

Art. 17 PV

Uitzondering !!!

- Recht op gegevenswissing blijft buiten toepassing indien dat de archivering met het oog op het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden onmogelijk dreigt te maken, of deze ernstig in het gedrang dreigt te brengen. (Art 17 sub d AVG)
- Echter: enkel indien bij de archivering passende waarborgen zijn genomen om de betrokkene te beschermen (Art. 89 AVG)
  - Overheidsorganisaties zijn daarom verplicht om technische en organisatorische maatregelen te treffen om het beginsel van dataminimalisatie te garanderen.

Vertegenwoordiging

- De betrokkene mag zich laten vertegenwoordigen door een belangenorganisatie. Deze organisatie mag namens hem een klacht indienen, naar de rechter stappen, of het recht op schadevergoeding uitoefenen.

- Klachtrecht bij rechtbank tegen toezichthouder

Art. 80 AVG

Uitzonderingen voor de overheid

Rechten van betrokkenen kunnen beperkt worden, met inachtneming van fundamentele rechten van betrokkenen, als dat nodig is voor:

- Nationale veiligheid;
- Strafrechtelijk onderzoek;
- Juridische procedures;
- Belangrijke doelen die de openbare orde dienen.

Art. 23 AVG

Uitzonderingen pseudonimisering

Kun je de betrokkene niet meer identificeren? Dan hoef je niet voldoen aan de verzoeken van de betrokkene

Tenzij

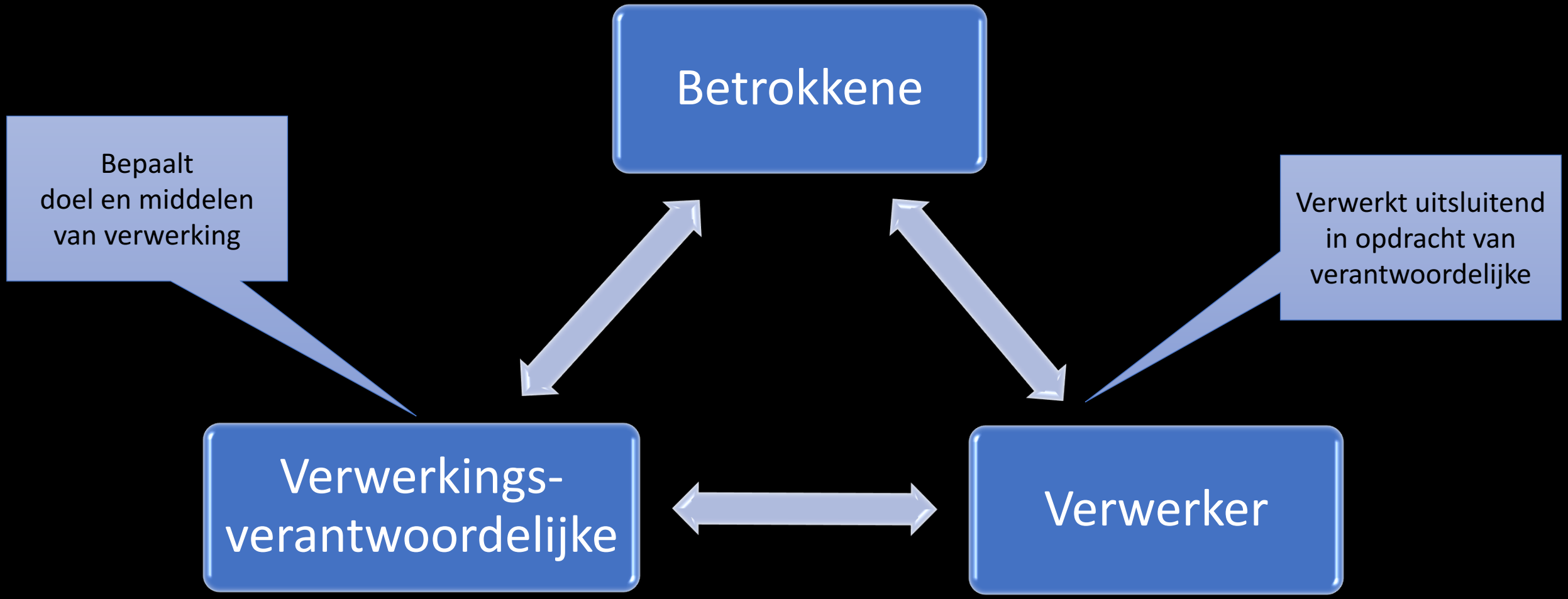
De betrokkene aanvullende gegevens verstrekt om identificatie mogelijk te maken.

Art. 11 AVG

Plichten van verwerkingsverantwoordelijken

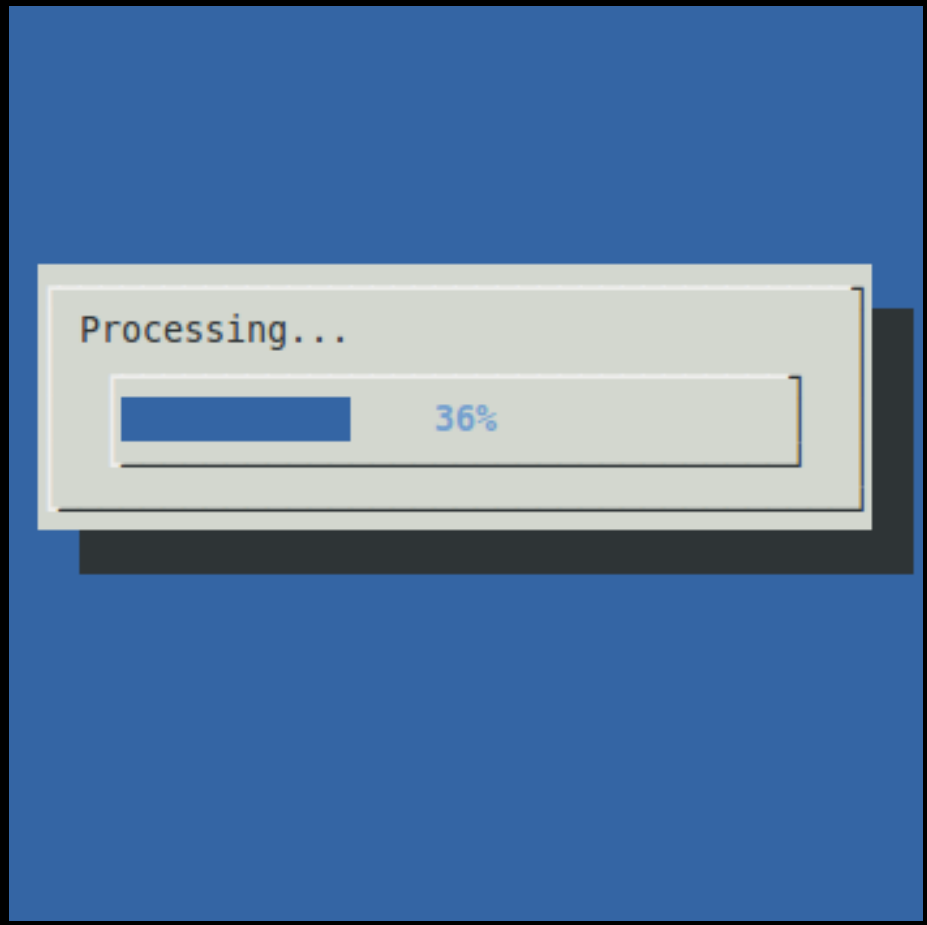
ICTRECHT

Terminologie en rollen



Verwerking

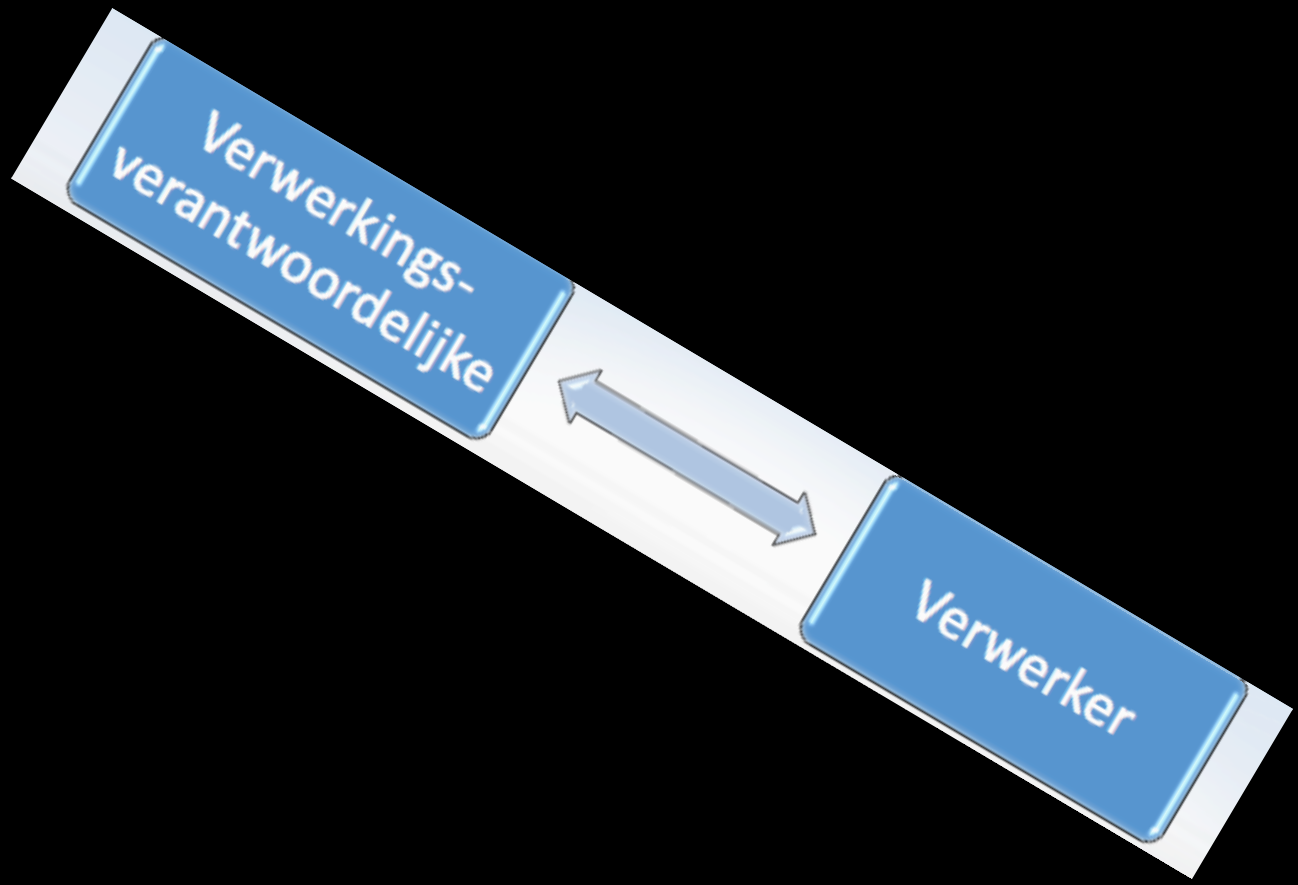
Een **bewerking** of een geheel van **bewerkingen** met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;



Art. 4 (2) AVG

Bewerkersovereenkomst

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 vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.



Art. 28 (1) AVG

Sub-verwerkers

- Inschakelen van derden mag alleen na toestemming verwerkingsverantwoordelijke
- Verwerker moet dezelfde verplichtingen uit de bewerkersovereenkomst doorzetten naar sub-verwerker
- Verwerker is volledig aansprakelijk voor het nakomen van de verplichtingen richting verwerkingsverantwoordelijke

Art. 28 AVG

Datalek?

- **Verlies:**
  - Verlies houdt in dat niemand de persoonsgegevens meer heeft;
  - Dat wil zeggen dat er ook geen complete en actuele **reservekopie** van de persoonsgegevens meer is.

- **Onrechtmatige verwerking:**
  - Aantasting van persoonsgegevens (blokkeren/versleutelen);
  - Onbevoegde kennisneming;
  - Wijziging van persoonsgegevens;
  - Verstrekking van persoonsgegevens;
  - **Ook als het niet uitgesloten kan worden!**

Informatieplicht (oa)

- Doel van de verwerking;
- Ontvangers van persoonsgegevens;
- Informatie over doorgifte naar derde landen buiten de EU;
- Bewaartermijnen/criteria bepalen termijn;
- Recht op inzage, correctie, verwijdering;
- Recht om toestemming in te trekken;
- Uitleg over de logica bij geautomatiseerde verwerking, gevolgen betrokkenen (profilering).

Art. 13 AVG

Uitzondering !!!

- Archivering = altijd toegestaan, ook als dat doel oorspronkelijk niet was gemeld aan de betrokkene.
- Betrokkene informeren over de verwerking? Niet nodig ivm onevenredig veel inspanning.
- Afwijken van uitgangspunt korte bewaartermijn?

Register verwerkingsverantwoordelijke

- Bijhouden (en kunnen tonen) van een register voor de gegevensverwerking
- Bevat oa:
  - de doeleinden van de gegevensverwerking
  - wie de betrokkenen zijn en welke categorieën persoonsgegevens er worden verwerkt
  - categorieën van ontvangers
  - welke bewaartermijnen er worden gehanteerd
  - een beschrijving van de beveiligingsmaatregelen

Art. 30 (1) AVG

Register

- Op verzoek aan toezichthouder tonen
- Niet van toepassing op organisaties < 250 medewerkers tenzij:
  - verwerking waarschijnlijk risico inhoudt voor rechten/vrijheden betrokkenen
  - de verwerking stelselmatig is, of
  - bijzondere persoonsgegevens worden verwerkt

Art. 30 AVG

Aanstellen functionaris voor gegevensbescherming

- Verwerking plaatsvindt door overheidsorgaan.
- ‘Core activity’ bestaat uit het stelselmatig en op grote schaal (meta) data over het gedrag verwerken.
- Er grootschalige verwerking van bijzondere persoonsgegevens plaatsvindt.

Art. 37-39 AVG

Taken functionaris

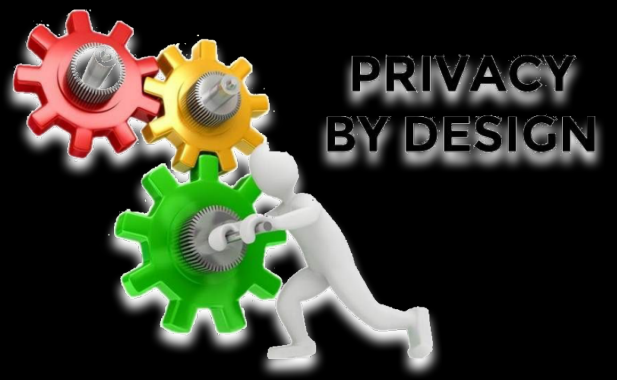
- Informeren en adviseren over verplichtingen
- Toezien op compliance
- Adviseren bij PIA’s
- Meewerken met toezichthouder
- Aanspreekpunt betrokkenen
- Incompatibiliteit

Art. 39 AVG

Privacy by design

- Passende technische en organisatorische maatregelen om gegevens te beschermen.
  - Gegevensminimalisatie
  - Beveiliging (bijvoorbeeld: Encryptie)
  - Juridische waarborgen

- Uitvoeren van een Privacy Impact Assessment (soms).



Privacy Impact Assessment

Een PIA is verplicht als:

- Geautomatiseerde besluitvorming ten aanzien van persoonsgegevens systematisch plaatsvindt (inclusief profiling);
- Op grote schaal bijzondere persoonsgegevens worden verwerkt;
- Openbare ruimten systematisch op grote schaal gemonitord worden;
- Vormen van verwerking die door de toezichthouder worden aangewezen, of waarvan de toezichthouder stelt dat een PIA **niet** hoeft.

Art. 35 lid 3 AVG

Inhoud

Een PIA bevat in ieder geval:

- Een omschrijving van de uit te voeren verwerkingen;
- Een beoordeling van noodzakelijkheid en proportionaliteit;
- Een risicoanalyse;
- Maatregelen ter preventie van de risico’s

Art. 35 lid 7 AVG

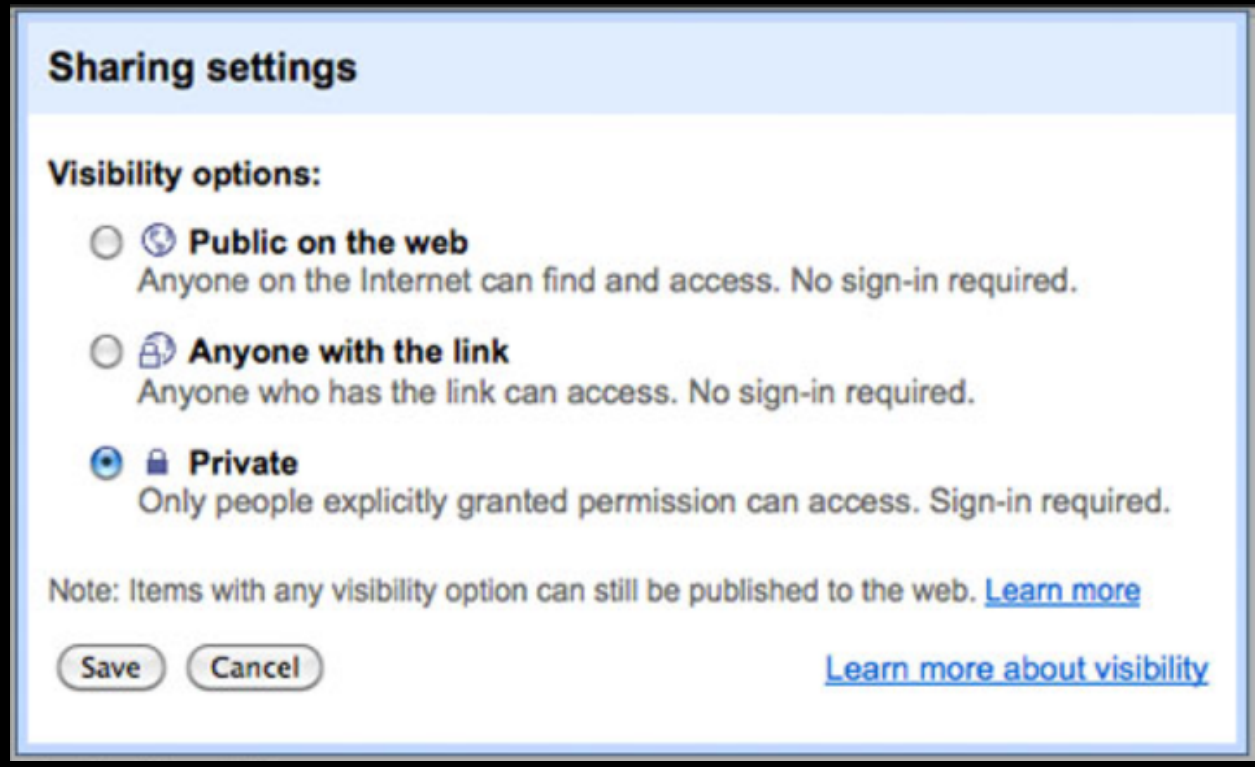
Consultatie

- Als uit de PIA blijkt dat er hoge risico's zijn die niet direct opgelost kunnen worden → verplichte consultatie bij de toezichthouder.
- Binnen acht weken reageert de toezichthouder.

Art. 36 AVG

Privacy by default

- Niet vragen indien niet relevant
- Niet meer bewaren dan nodig
- Wissen zodra overbodig
- Alle instellingen standaard op de meest beperkte optie



Art. 25 lid 2 AVG

Sancties

- Nationale en Europese toezichthouder.
- Schriftelijke waarschuwing
- Regelmatige audits
- Boete tot het maximum van
  - € 20.000.000
  - 4% van wereldwijde jaaromzet

Art. 83 AVG

Schadevergoeding (civiele handhaving)

- Materiële of immateriële schade
- Meerdere verantwoordelijken of bewerkers betrokken bij verwerking? Dan ieder voor de gehele schade aansprakelijk

Art. 82 AVG

Vragen?

Mr. Dr. Mathieu Paapst CIPM

Juridisch adviseur, Certified information privacy manager

m.paapst@ictrecht.nl

050-2093499

ICTRECHT

One slide to rule them all

1. Harmonisatie;
2. Begrip ‘persoonsgegevens’ wordt uitgewerkt;
3. Toestemming wordt strenger;
4. Meer rechten, zoals beperken en bezwaar maken
5. (in sommige gevallen) verplicht aanstellen van een FG;
6. Aanmelden gegevensverwerking vervalt;
7. Eisen aan bewerkersovereenkomst worden ingevuld;
8. In sommige gevallen moet een PIA uitgevoerd worden;
9. Privacy by design & default worden opgenomen in de wet;
10. Europese toezichthouder en verhoging boetemaximum.

Wat te doen in 2017?

- Budget voor data inventarisatie
  - Welke data is er (input/output) en met welk doel
  - Welke (derde) partijen werken er mee?
  - Bewaartermijn?
- Budget voor privacy by design and default
  - Toekomstige data collectie (eventueel uitvoeren PIA)
  - Oplossen legacy datasets
- Budget voor uitoefening rechten betrokkene
  - Recht tot verwijdering, dataportabiliteit, beperkingen

- Budget voor beveiliging
  - encryptie
- Budget voor het opzetten van het privacyprogramma
  - Coördineren en aanjagen AVG implementatie
  - Workshops en trainingen.
  - Controle en invoeren juridische waarborgen (oa bewerkersovereenkomsten, geheimhoudingsovereenkomsten, byod beleid, email beleid)
- Budget voor de inhuur van een Data Protection Officer /FG
  - Uiterlijk mei 2018