

De nieuwe privacyverordening in 1 slide per minuut

Mr. dr. Mathieu Paapst

m.paapst@ictrecht.nl / 050-2093499



Wie ben ik



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.



Persoonsgegevens

Persoonsgegevens

Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

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 identifier zoals een naam, een **identificatienummer**, **locatiegegevens**, een **online identifier** of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

Bijzondere persoonsgegevens

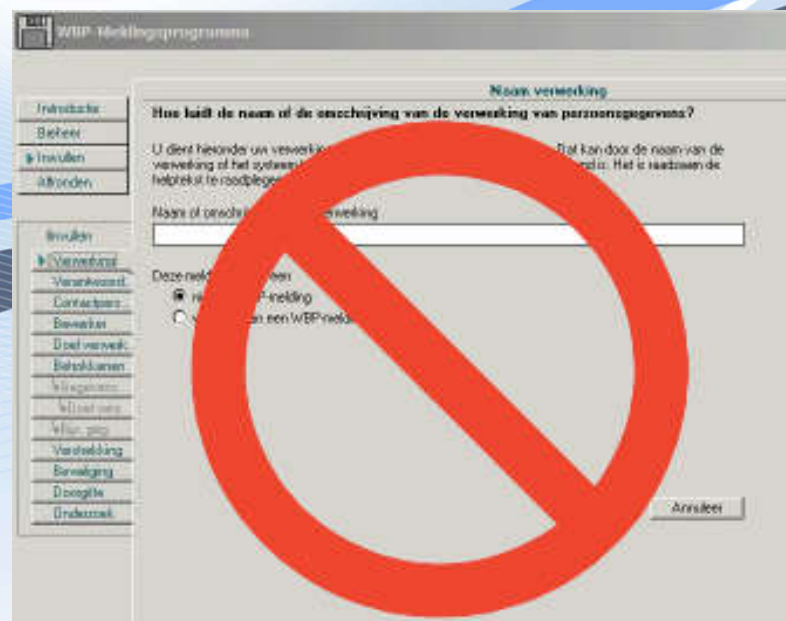


...waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of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

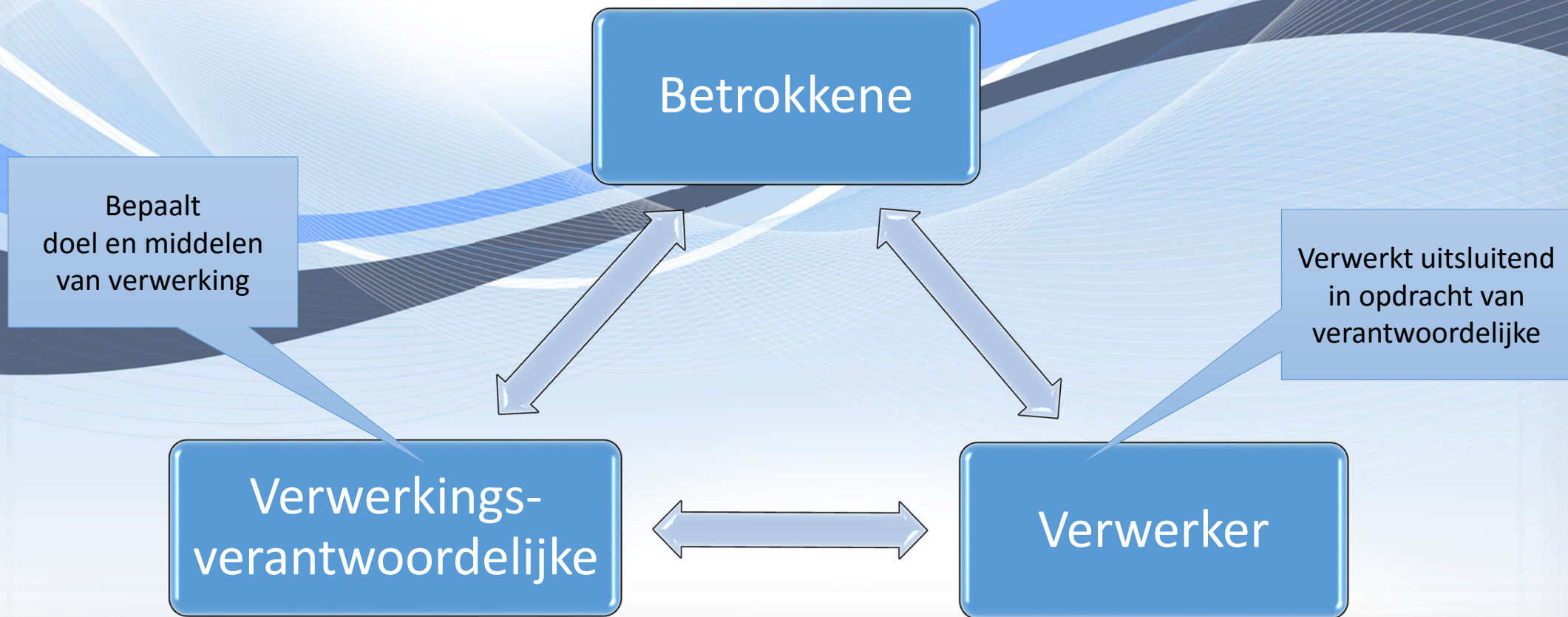
Niet langer dan nodig



Aanmelden verwerking



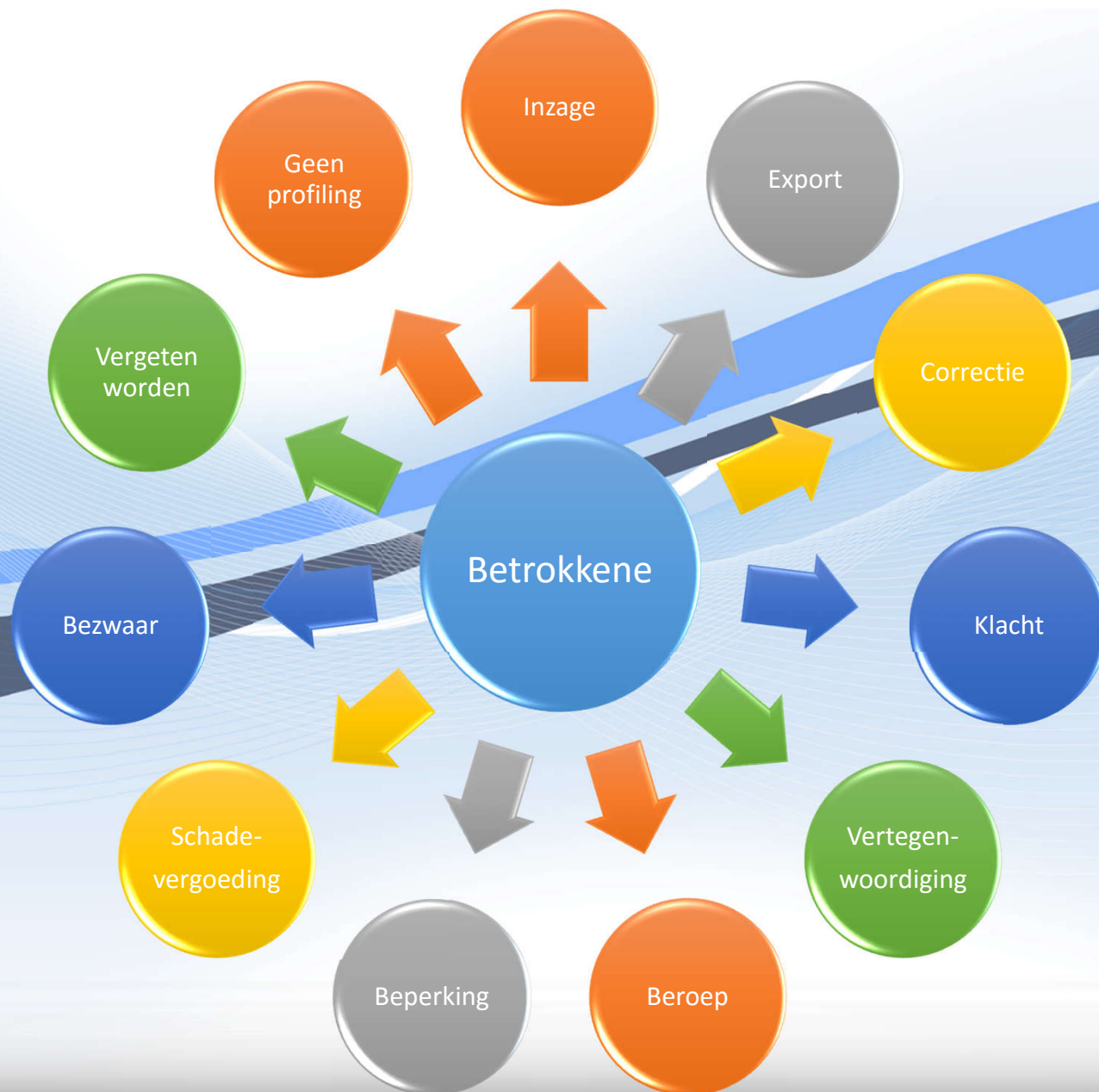
Terminologie en rollen



Rechten van betrokkenen

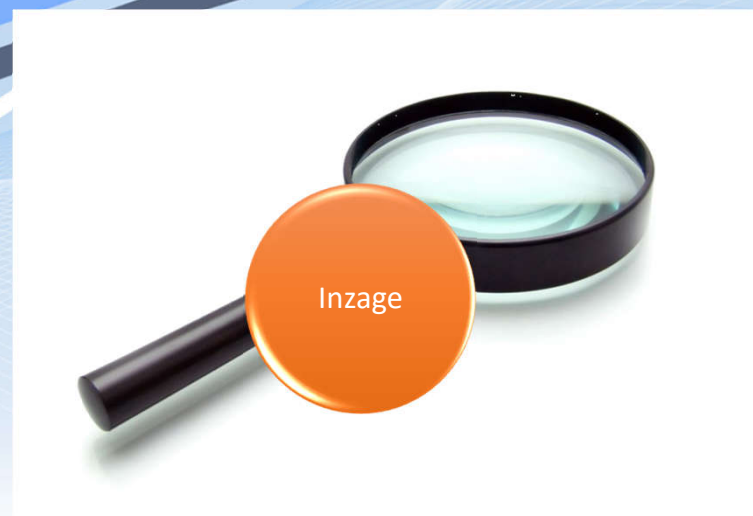


ICTRECHT



Recht van inzage

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



Export

Betrokkene moet in kennis gesteld worden van naleving artikel 46 bij export van persoonsgegevens



Recht van data-export

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

Alleen als:

- Verwerking is gebaseerd op 'toestemming' of 'uitvoering overeenkomst'; en
- Verwerking geautomatiseerd plaatsvindt
- Er geen rechten van derden worden geschaad

Recht van portabiliteit

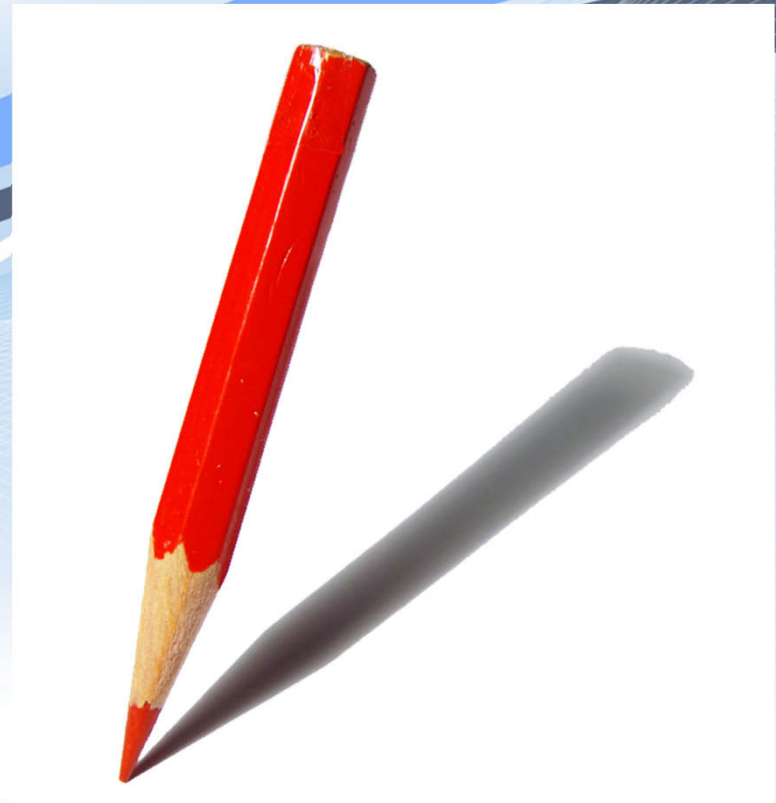
NIEUW

“...heeft de betrokkene het recht dat de persoonsgegevens, indien dit technisch mogelijk is, rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere worden doorgezonden.”



Correctie en rectificatie

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





Restrictie

„beperken van de verwerking”:
het markeren van opgeslagen
persoonsgegevens met als doel de
verwerking ervan in de toekomst
te beperken;

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

Restrictie

Als de verwerking eenmaal is beperkt mogen de persoonsgegevens, met uitzondering van de opslag daarvan, uitsluitend verwerkt worden met toestemming van de betrokkene.



Kennisgeving

De verwerkingsverantwoordelijke stelt alle ontvangers in kennis van rectificatie of wissing van persoonsgegevens of beperking van de verwerking.

Tenzij dit onmogelijk is of onevenredig veel inspanning vergt.





Vertegenwoordiging

De betrokkene mag zich laten vertegenwoordigen door een belangenorganisatie. Deze organisatie mag namens hem een klacht indienen of het recht op schadevergoeding uitoefenen.



Klacht

“...heeft iedere betrokkene het recht een klacht in te dienen bij een toezichthoudende autoriteit, met name in de lidstaat waar hij gewoonlijk verblijft, hij zijn werkplek heeft of waar de beweerde inbreuk is begaan, indien hij van mening is dat de verwerking van hem betreffende persoonsgegevens inbreuk maakt op deze verordening.”



Schadevergoeding

- Materiële of immateriële schade
- Verwerkingsverantwoordelijke is aansprakelijk door hem veroorzaakte schade door verwerkingen die inbreuk maken op de AVG
- Een verwerker is slechts aansprakelijk voor schade ontstaan door zijn onrechtmatig handelen.



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:

Verwijdering

- Verwijdering en staking van gebruik, ook door derden
- 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

Recht op gegevenswissing („recht op vergetelheid”)

“Dat recht is met name relevant wanneer de betrokkene toestemming heeft gegeven als kind, toen hij zich nog niet volledig bewust was van de verwerkingsrisico's, en hij dergelijke persoonsgegevens later wil verwijderen, met name van het internet. De betrokkene dient dat recht te kunnen uitoefenen niettegenstaande het feit dat hij geen kind meer is.”

Geautomatiseerd besluit

🕒 26 augustus 2015 06:00

Letter achter je huisnummer? Verzekering 100 euro duurder



Verzekeraars laten de premie voor inboedel- en autoverzekeringen steeds vaker afhangen van de woonplaats van hun klant. Sommige verzekeraars gaan zelfs zo ver dat bij een huisnummertoevoeging (zoals A of -2) de premie tientallen euro's hoger uitvalt.

- Niet zomaar toegestaan
- Menselijke tussenkomst
- Informatieplicht: uitleg totstandkoming besluit

Wel als:

- Uitvoering overeenkomst
- Uitvoering wettelijke plicht
- Toestemming

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.



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.

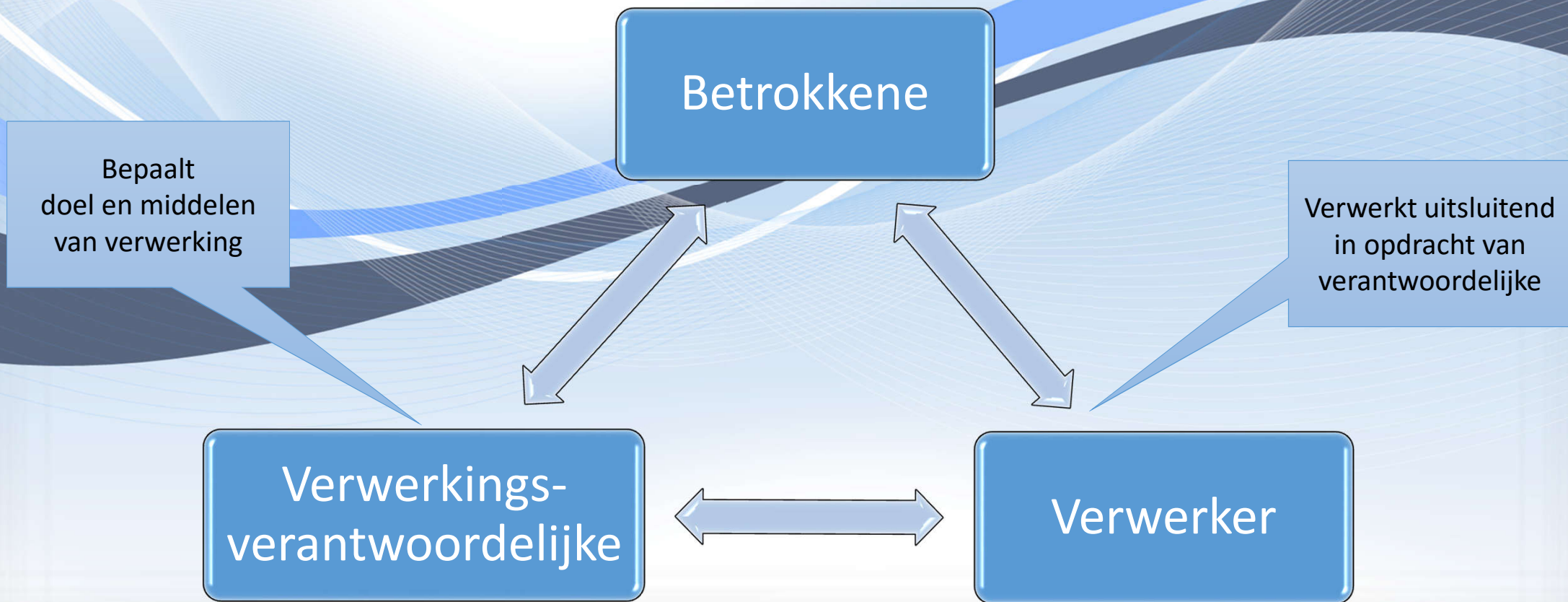


Plichten van verwerkingsverantwoordelijken



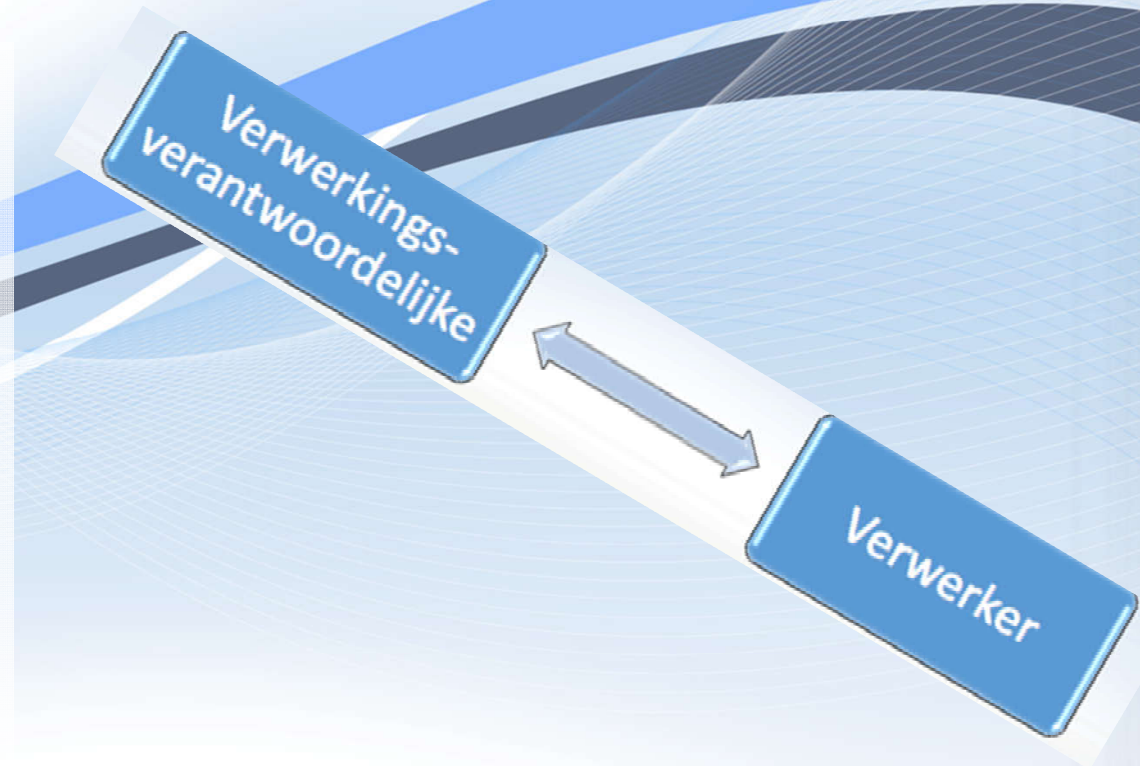
ICTRECHT

Terminologie en rollen



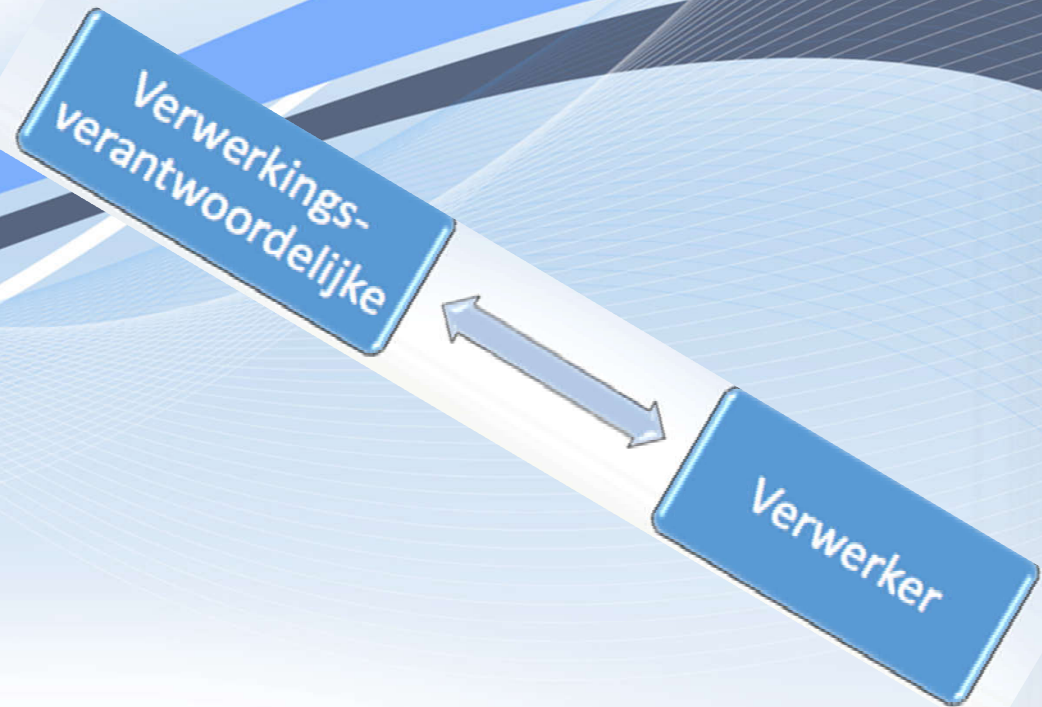
Bewerkersovereenkomst

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.



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
- Indien verwerker de doeleinden en middelen gaat bepalen, wordt de verwerker als verwerkingsverantwoordelijke beschouwd



Register verwerkingsverantwoordelijke

- Bijhouden van een register voor de gegevensverwerking
- Bevat oa:
 - wie de functionaris gegevensbescherming is
 - 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



Register

- Schriftelijk, inclusief elektronisch
- 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



Informatieplicht

- Identiteit van de verwerkingsverantwoordelijke;
- Functionaris voor gegevensbescherming;
- Doel van de verwerking;
- Wettelijke grondslag (indien van toepassing: de gerechtvaardigde belangen waarop de verwerking wordt gebaseerd);
- Ontvangers van persoonsgegevens;
- Melden als gegevens voor ander doel worden verwerkt dan waarvoor ze zijn verkregen
- Informatie over doorgifte naar derde landen;
- Bewaartermijnen/criteria bepalen termijn;
- Recht op inzage, correctie, verwijdering;
- Recht om toestemming in te trekken;
- Verplichting betrokkene persoonsgegevens te verstrekken en wat de gevolgen zijn indien dit niet gebeurt (in het kader contractuele verplichting/wettelijke plicht);
- Recht om een klacht bij de toezichthouder in te dienen;
- Uitleg over de logica bij geautomatiseerde verwerking, gevolgen betrokkenen (profilering).

Vóórdat de gegevens verzameld worden!



Aanstellen functionaris voor gegevensbescherming

Verplicht om aan te stellen als:

- Verwerking plaatsvindt door overheidsorgaan
- 'Core activity' bestaat uit verwerkingen die stelselmatige observatie op grote schaal van betrokkenen vereisen
- Er grootschalige verwerking van bijzondere persoonsgegevens plaatsvindt



Taken functionaris

- Informeren en adviseren over verplichtingen
- Toezien op compliance, inclusief audits en trainingen aan staf
- Adviseren bij PIA's
- Meewerken met toezichthouder
- Aanspreekpunt toezichthouder



Adequate beveiliging

Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

Passend, zoals

- Pseudonimisering en encryptie;
- Vertrouwelijkheid, beschikbaarheid en integriteit waarborgen;
- Adequaat en tijdig kunnen reageren op incidenten;
- Regelmatig testen, evalueren en bijschaven.

Gedragcode of certificering

3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.



Meldplicht datalekken

- Staat nu ook al in de wet.
- “Inbreuk in verband met persoonsgegevens”.
- Inbreuken binnen 72 uur (!) melden, tenzij de inbreuk geen risico inhoudt voor de rechten en vrijheden van natuurlijke personen.
- De verwerkingsverantwoordelijke documenteert alle inbreuken.
- Voor hoelang?
- Bewerkers moeten alle incidenten aan hun klanten gaan melden (art. 33 lid 2)

Geen meldplicht

Een melding aan de **betrokkenen** is niet nodig als verantwoordelijke **passende technische beschermingsmaatregelen** heeft genomen waardoor de persoonsgegevens die het betreft **onbegrijpelijk of ontoegankelijk** zijn voor eenieder die geen recht heeft op kennisname van de gegevens.

Wél meldplicht

Indien (waarschijnlijk) ongunstige gevolgen voor betrokkenen:

- Persoonsgegevens van gevoelige aard;
- Onrechtmatige publicatie;
- Aantasting in eer en goede naam;
- (identiteits)fraude;
- Discriminatie;
- Financiële schade.



Let op: ook versleutelde data kan worden vernietigd of aangetast en daardoor ongunstige gevolgen voor de betrokkene hebben. Dus ook in dat geval moet de betrokkene daarover ingelicht worden.

Privacy by Design

Privacy geïntegreerd in het ontwerp (door technische en organisatorische maatregelen)

Privacy by Design ontwikkelt het inzicht dat privacy in de toekomst niet slechts kan worden gewaarborgd door uitsluitend het naleven van wettelijke kaders, maar dat de verzekering van privacy in eerste instantie moet komen van een standaard wijze van opereren binnen organisaties.

Privacy by design

Beginselen van een 'privacyproof' systeem:

- Creëer draagvlak;
- Minimalisatie van gegevens;
- Transparant naar buiten toe;
- Risico's met betrekking tot veiligheid in kaart brengen.

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.

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



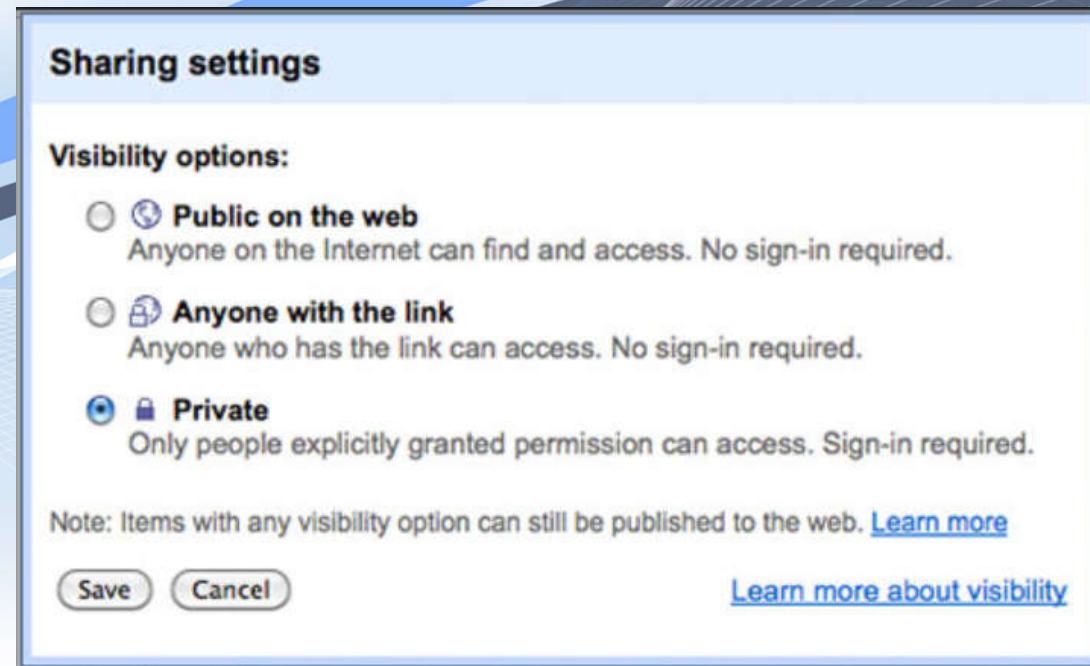
Consultatie

- 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.



Privacy by default

- Niet vragen indien niet relevant
- Niet meer bewaren dan nodig
- Wissen zodra overbodig
- Alle instellingen standaard op de meest beperkte optie
- Alle privacy-zaken via controlepaneel of helpdesk te beheren door de betrokkene



Wanneer is de wet van toepassing?

- Indien de verwerkingsverantwoordelijke of de verwerker in de EU is gevestigd
- Indien het om persoonsgegevens van betrokkenen uit de EU gaat, en de activiteiten van de verantwoordelijke zien op:
 - Aanbieden van goederen of diensten (ongeacht betaling)
 - Monitoren van gedrag



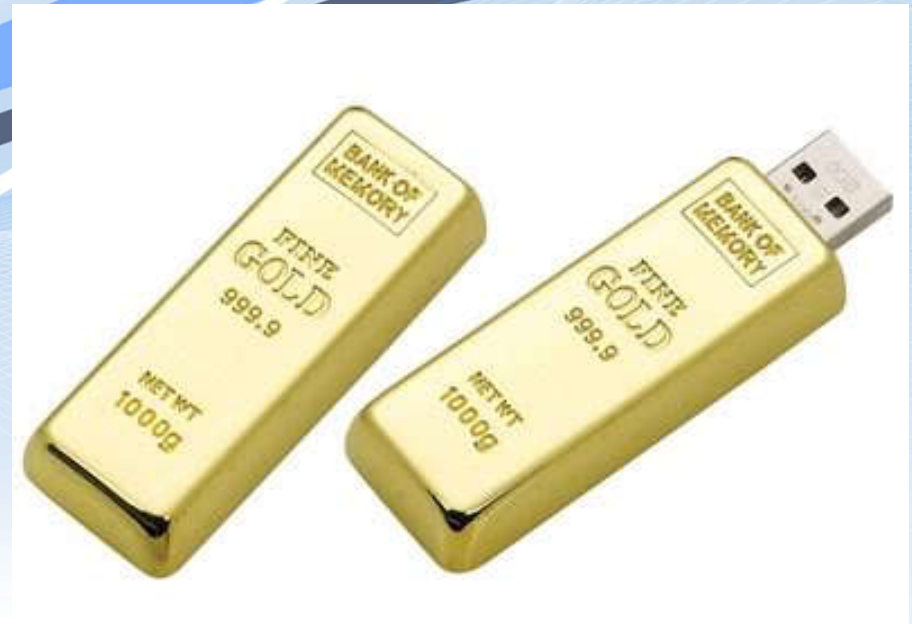
Sancties

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



Civiele handhaving

- Tegen verantwoordelijke of bewerker bij inbreuk rechten
- Klachtrecht bij rechtbank tegen toezichthouder indien geen adequate afhandeling klacht, of indien beslissing toezichthouder gevolgen heeft voor betrokkene
- Bevoegde rechtbank
 - Waar verantwoordelijke of bewerker is gevestigd
 - Waar betrokkene woont
 - Waar toezichthouder gevestigd is
- Recht op compensatie voor geleden schade



Inwerkingtreding



ICTRECHT

Richtlijn vs Verordening

Richtlijn

- Instructie aan lidstaten
- Om te zetten in wetgeving
- Nationale afwijkingen mag tenzij volledige harmonisatie

Verordening

- Rechtstreekse werking
- In alle lidstaten direct verbindend
- Geen nationale afwijkingen tenzij in verordening toegestaan



Brussels, 15 December 2015
(OR. en)

15039/15

Interinstitutional File:
2012/0011 (COD)

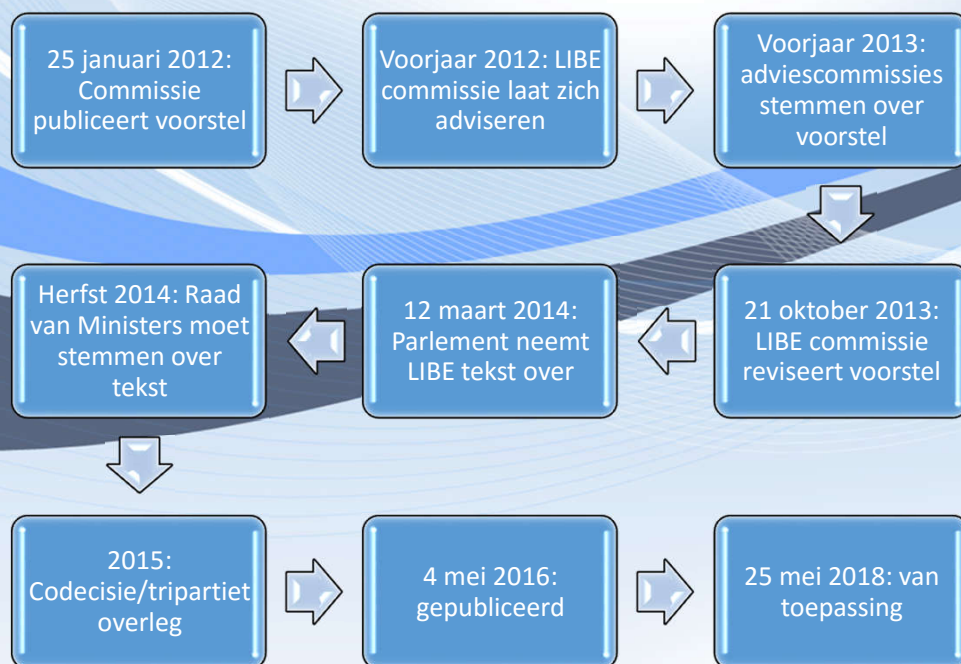
LIMITE

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

Tijdslijn 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

Vragen?

Mathieu Paapst

Juridisch adviseur, CIPM

m.paapst@ictrecht.nl

050-2093499



ICTRECHT