DE ALGEMENE VERORDENING GEGEVENSBESCHERMING

Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University, Netherlands
www.bartvandersloot.nl

OVERZICHT

(1) Wanneer is de AVG op je organisatie van toepassing?

(2) Welke uitgangspunten gelden er voor de AVG?

(3) Welke plichten gelden er als de AVG van toepassing is?

(4) Welke rechten hebben datasubjecten?

(5) Waarom is het belangrijk om de regels uit de AVG te volgen?

GEGEVENSBESCHERMING ≠ PRIVACY

HANDVEST VAN DE GRONDRECHTEN VAN DE EUROPESE UNIE

Artikel 7 Eerbiediging van het privé-leven en het familie- en gezinsleven

Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.

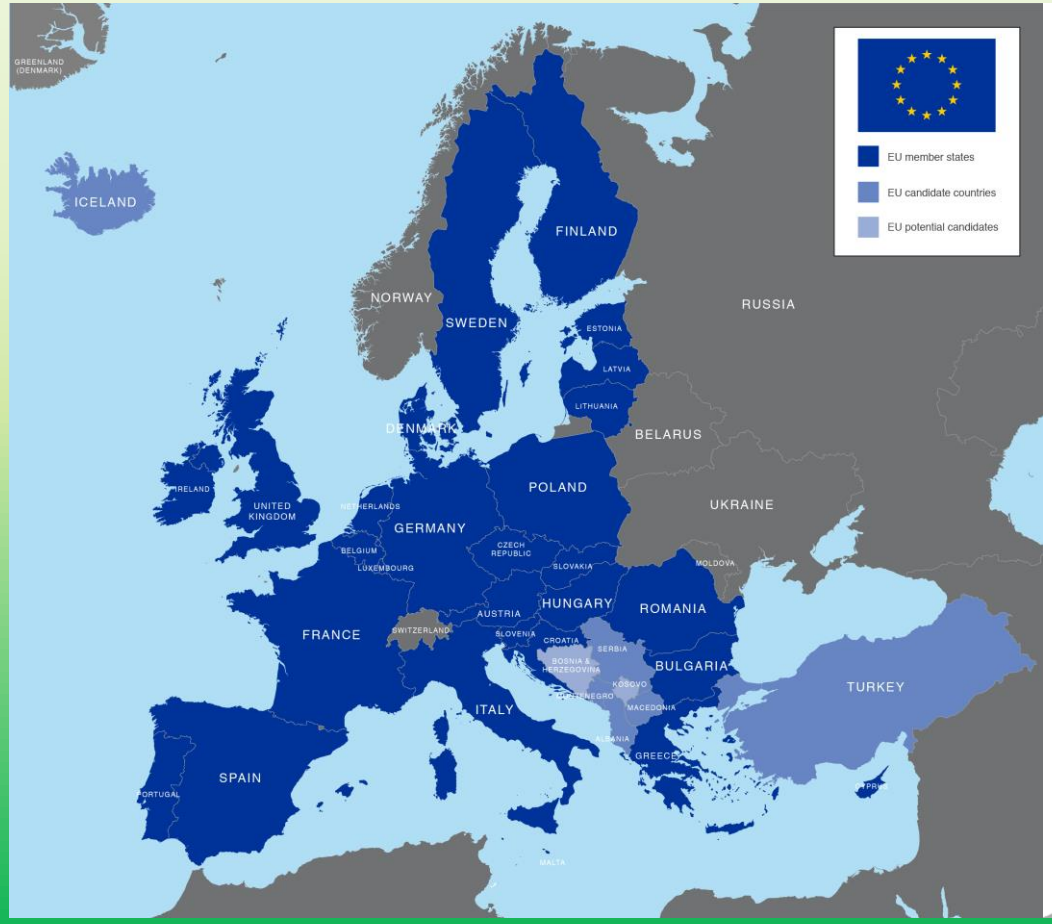
Artikel 8 Bescherming van persoonsgegevens

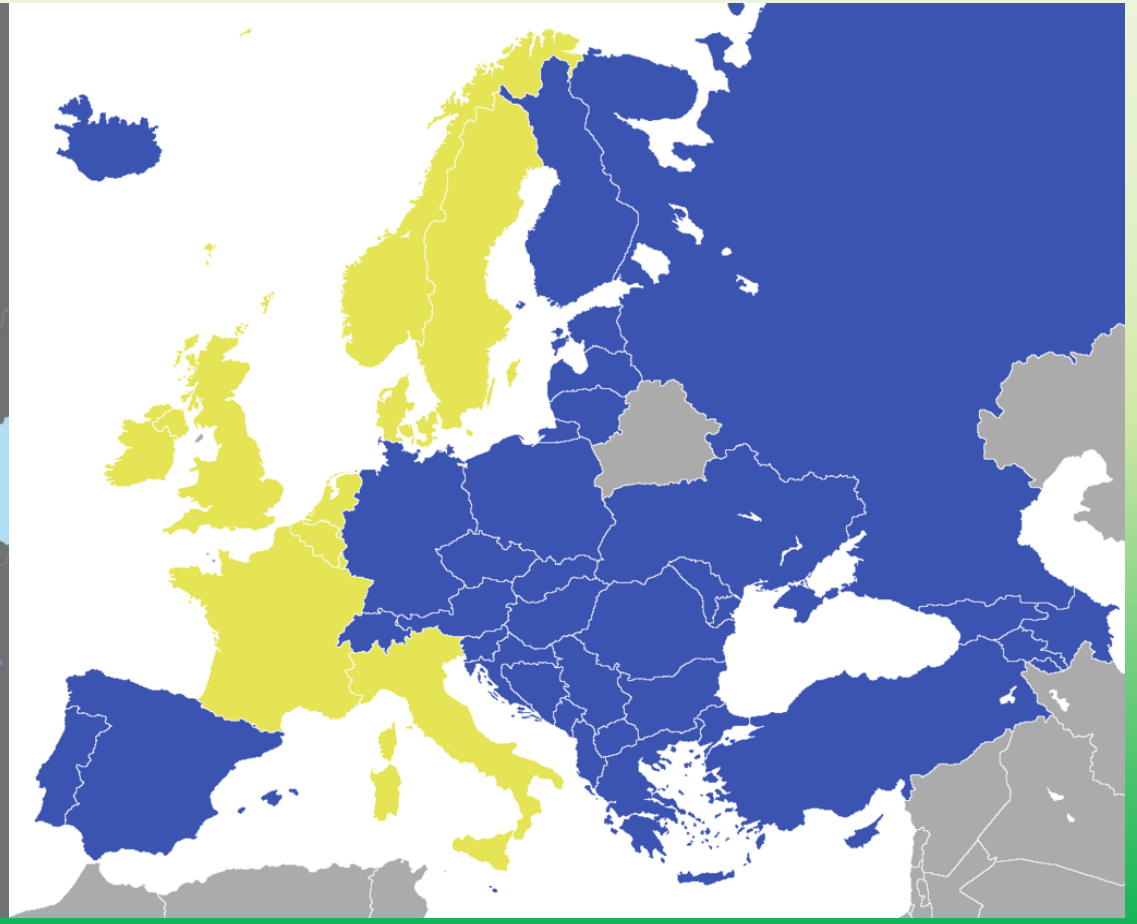
1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

EUROPA ≠ EUROPESE UNIE ≠ RAAD VAN EUROPA





WAAROM IS ER DE AVG?

Er waren vijf problemen die moesten worden aangepakt

1. Verschillende implementatie in EU landen
2. Verschillen in handhaving in EU landen
3. Zwakke handhavingsmogelijkheden
4. Handhavingstaak lag bij de Data Protection Authorities, in Nederland de Autoriteit Persoonsgegevens
5. Individuen weten vaak niet dat hun data worden verwerkt en ervaren weinig controle

WAAROM IS ER DE AVG?

Daarom zijn er vijf oplossingen:

1. Een Verordening heeft in tegenstelling tot een Richtlijn direct effect
2. Er kan samen worden gewerkt tussen handhavende organisaties
3. Er kunnen hoge boetes en sancties worden opgelegd
4. Meer plichten voor dataverwerkende organisaties om aan interne controle en auditing te doen
5. Individuen krijgen meer controlemogelijkheden over hun data

(1) WANNEER IS DE AVG OP JE ORGANISATIE VAN TOEPASSING?

1. Als er ‘persoonsgegevens’
2. Worden ‘verwerkt’
3. Door een ‘verantwoordelijke’
4. Op EU grondgebied

5 En er geen uitzondering van toepassing is

1.1 PERSOONSGEGEVEN

Een persoonsgegeven is een gegeven waarmee je iemand kan identificeren.

Dat kan zijn een **direct persoonsgegeven of een indirect persoonsgegeven**. Een direct persoonsgegeven is bijvoorbeeld iemands naam. Een indirect gegeven is een specifiek detail aan iemand, bijvoorbeeld: 'het zeilmeisje wilde de hele wereld over, maar de rechter verbood het haar'. In dit verband is 'het zeilmeisje' voldoende om iemand, namelijk Laura Dekker, te identificeren.

Het gaat zowel om **privé als publieke gegevens**. Ook de term 'die persoon daar, naast de lantaarnpaal, met de oranje stropdas' is dus een persoonsgegeven. Of het gegeven dus publiekelijk toegankelijk en openbaar is of niet, of het gegeven een feit van algemene bekendheid is of niet, een gegeven zal als 'persoonsgegeven' hebben te gelden als er iemand mee geïdentificeerd kan worden. Daarvoor is het niet nodig dat je ook de naam van de persoon met de oranje stropdas weet.

Het gaat om **gevoelige informatie** (Meneer De Wit heeft prostaatkanker), maar een persoonsgegeven kan ook **hele gewone informatie** bevatten - zoals het feit dat iemand een oranje stropdas omheeft. De gevoeligheid van een gegeven doet er in dit opzicht dus niet toe – wel is het zo dat bij de verwerking van gevoelige gegevens aan meer voorwaarden moet worden voldaan.

Het gaat om **identificerende gegevens**, maar ook om **identificeerbare gegevens**. Die laatste zijn bijvoorbeeld gegevens die op dit moment nog niemand identificeren, maar dat op termijn wel kunnen doen. Stel, je hebt bijvoorbeeld twee databases die op zichzelf niemand uniek kunnen identificeren, maar als ze worden samengevoegd wel, dan kan het zijn dat ook de afzonderlijke databases moeten worden gezien als bevattende persoonsgegevens.

Er is een trend om niet alleen de '**identificeerbaarheid**' van gegevens centraal te stellen, maar ook de '**individualiseerbaarheid**' van mensen. Stel, je hebt een profiel van iemand gemaakt, bijvoorbeeld door informatie die je online verzamelt via cookies, maar je weet niet precies wie het is. Toch kan je die persoon wel individueel tracken en daarop bepaalde handelingen ondernemen, zoals het aanbieden van gepersonaliseerde advertenties of content. Dan vallen de gegevens in principe ook onder het begrip 'persoonsgegeven'.

Encryptie van gegevens – omdat gegevens worden geëncrypteerd en niemand anders de digitale sleutel heeft, zijn de gegevens voor anderen onleesbaar. Daarom zijn de gegevens geen persoonsgegevens, zo is het argument. Dat klopt echter niet. Deze gegevens zijn in ieder geval nog door jou/je organisatie leesbaar en dus als persoonsgegeven aan te merken. Ook is decryptie, het omgekeerde proces van encryptie, vaak mogelijk. Hackers worden hier steeds beter in en er is bijna geen code die niet gekraakt kan worden. Daarom betekent het encrypteren van data niet dat je geen persoonsgegevens verwerkt

Het gebruik van pseudoniemen – in de dataset staat niet de naam van een klant of een derde, maar een persoonlijke code. 'Mevrouw De Bruijn' wordt dus '245X*!LK9' of 'Sneeuwwitje'. Wederom is dit een goede techniek om in te zetten om aan de beveiligingseisen van de Verordening te voldoen, maar het betekent niet dat er geen persoonsgegevens worden verwerkt. Een pseudoniem is immers ook een uniek gegeven en ook zonder naam zal een dataset doorgaans iemand kunnen identificeren.

Het anonimiseren van gegevens. Als persoonsgegevens inderdaad worden geanonimiseerd, dan is het gegevensbeschermingsrecht inderdaad niet van toepassing. Anoniem betekent immers dat de gegevens niet meer tot een persoon te herleiden zijn. Bedenk hierbij wel dat vaak het omgekeerde proces, het de-anonimiseren, ook mogelijk is. Zelfs bij medische data van patiënten die voor onderzoek werden gebruikt, zwaar waren geanonimiseerd en waarvan alle identifyers waren gestript blijkt uit experimenten dat bij een fors deel toch een persoon kan worden ge-reïdentificeerd. Als dit inderdaad mogelijk is, dan zijn gegevens eigenlijk helemaal niet anoniem en hebben de gegevens dus toch gewoon als persoonsgegevens te gelden. Eén van de meest gehoorde adagia in dit verband is: 'data can either be valuable, or fully anonymous, but never both.'

Het aggregeren van data. De data worden gelijk op een grote hoop gegooid en alleen per categorie geanalyseerd, met een *n* van zeg groter dan 100. Ook bij zulke grote categorieën is het in principe waar dat de Verordening niet van toepassing is. Het gegevensbeschermingsrecht is immers primair gericht op de bescherming van het individu, het data subject. Stel je toch drie vragen:

- (1) Aggregeer ik alle persoonsgegevens?
- (2) Zijn de data nooit persoonsgegevens geweest?
- (3) Gebruik je algemene profielen om klanten specifiek te benaderen?

1.2 VERWERKT

Er is slechts één handling die hier mogelijk niet onder valt en dat is het puur passief doorvoeren van persoonsgegevens. Stel bedrijf A gevestigd in Amsterdam, verstuurt persoonsgegevens naar bedrijf B gevestigd in Rotterdam, via de servers van cloudprovider C gevestigd in Utrecht. Als C verder niets doet met de gegevens – ook niet cached – maar allen als doorgeefluik fungeert, dan is de Verordening meestal niet op hem van toepassing. Op A en B natuurlijk wel. Kortom, bijna alles wat je doet met data valt onder verwerking in juridische zin.

1.3 DE VERANTWOORDELIJKE

Vaak zal een organisatie of persoon worden aangemerkt als ‘verantwoordelijke’ voor de gegevensverwerking. Om vast te stellen of iemand een ‘verantwoordelijke’ is gelden globaal twee criteria. De verantwoordelijke is degene die het doel van de gegevensverwerking bepaalt – bijvoorbeeld voor het mailen van klanten, voor het verbeteren van de website of voor het ontwikkelen van nieuwe producten – en degene die de middelen vaststelt – dit criterium heeft betrekking op hoe de gegevens worden verzameld en verwerkt, met welke methoden en met behulp van welke technieken en software ze worden geanalyseerd.

- De verantwoordelijke moet aan alle plichten en verantwoordelijkheden uit de Verordening voldoen.
- De verantwoordelijke moet er voor zorgen dat degenen die namens hem gegevens verwerken ook aan alle plichten uit de Verordening voldoen.
- De verantwoordelijke moet er voor zorgen dat gegevens alleen naar organisaties in andere landen worden verstuurd als daar de regels uit de Verordening worden gerespecteerd

1.3 DE VERANTWOORDELIJKE

Als bedrijf B samen met een andere organisatie, bedrijf C, de doelen en de middelen vatstelt, of bedrijf B het doel vaststelt en bedrijf C gaat over hoe en op welke wijze persoonsgegevens worden verwerkt, dan zijn bedrijven B en C doorgaans beide als ‘verantwoordelijke’ aan te merken. Dat betekent dat zij een gezamenlijke verantwoordelijkheid hebben om aan alle bepalingen uit de Verordening te voldoen.

1.4 EU RECHT IS VAN TOEPASSING

1. De algemene regel is dat de Verordening van toepassing is als de persoonsgegevens worden verwerkt door een verantwoordelijke of een verwerker ‘in het kader van een activiteit van een vestiging die in de EU is gevestigd’. Een activiteit is bijvoorbeeld het aanbieden van producten of diensten aan EU burgers.

2. Als de organisatie geen vestiging heeft in de EU, maar wel producten of diensten aanbiedt aan EU burgers en gegevens over hen verzamelt. Bijvoorbeeld een Amerikaans bedrijf, zonder vestiging in de EU, dat via een website EU burgers benadert. Of een product of dienst wordt aangeboden aan EU burgers hangt af van de situatie.

3. Als de organisatie niet in de EU is gevestigd, maar wel het gedrag van EU burgers monitort, voor zover die gedragingen plaatsvinden in de EU.

4. Ambassades en andere internationaalrechtelijke organisaties hebben een bijzondere status.

1.5 ER IS GEEN UITZONDERING VAN TOEPASSING

1. Veiligheidsdiensten en politie
2. Puur persoonlijke doeleinden
3. Speciale regels voor bijvoorbeeld vrijheid van meningsuiting en archivering

2. DE UITGANGSPUNTEN VAN HET GEGEVENSBESCHERMINGSRECHT

1. Mensenrechtenkader
2. Fair Information Principles (FIPS)
3. Legitieme grond voor verwerking
4. Legitieme grond voor verwerking bijzondere persoonsgegevens
5. Legitieme grond voor doorvoer van gegevens

2.1 MENSENRECHTENKADER

1. Noodzakelijkheid
2. Proportionaliteit
3. Subsidiariteit
4. Effectiviteit
5. Legitimiteit

2.2 FIPS

1. Dataminimalisatie
2. Specifiek doel
3. Doelbinding
4. Datakwaliteit
5. Dataveiligheid
6. Transparantie

2.3 LEGITIEME VERWERKINGSGRONDSLAG

1. Toestemming

2. Contract

3. Wettelijke grondslag

4. Bescherming van het datasubject

5. Publiek belang

6. f)de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

2.4 BIJZONDERE PERSOONSGEGEVENS

Verwerking van 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 zijn verboden. Tenzij:

1. Expliciete toestemming
2. het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht
3. vitale belangen van de betrokkene
4. instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam
5. persoonsgegevens zijn door de betrokkene openbaar gemaakt
6. uitoefening of onderbouwing van een rechtsvordering
7. zwaarwegend algemeen belang
8. preventieve of arbeidsgeneeskunde
9. volksgezondheid
10. wetenschappelijk of historisch onderzoek of statistische doeleinden

2.5 LEGITIEME GRONDSLAG OM GEGEVENS DOOR TE VOEREN

1. Beslissing van de Europese Commissie
   - Andorra, Argentina, Canada
   - Faeroe Islands, Guernsey, Israel,
   - Isle of Man, Jersey, New Zealand,
   - Switzerland *United States of America*
   - Eastern Republic of Uruguay

2. Passende waarborgen
   - Contractuele afspraken
   - Codes of Conducts
   - Certificeringsregels
   - Bindende bedrijfsregels

3. Uitzonderingen voor specifieke omstandigheden

3. PLICHTEN VAN ORGANISATIES

1. Documentatieplicht

2. Transparantie
   - Meldplicht datalekken

3. Beveiliging Persoonsgegevens
   - Technische veiligheid
   - Organisatorische veiligheid
   - Data Protection by Design
   - Data Proteciton by Default

4. Data Protection Officer

5. Data Protection Impact Assessement

4. RECHTEN VAN DATASUBJECTEN

1. Recht op informatie
2. Recht op rectificatie
3. Recht op verzet
   - Recht van bezwaar
   - Recht op vergetelheid
   - Recht op beperking van de verwerking
4. Recht op dataportabiliteit
5. Recht op verzet tegen profiling

(5) WAAROM IS HET BELANGRIJK OM DE REGELS UIT DE AVG TE VOLGEN?

1. Klanvriendelijkheid/uitstraling
2. Reputatieschade bij fouten
3. Klanten/partners die weglopen
4. Betrouwbaarheid gegevens en gegevensanalyse
5. Sancties: administratieve geldboeten kunnen oplopen tot 20 000 000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

(5) WAAROM IS HET BELANGRIJK OM DE REGELS UIT DE AVG TE VOLGEN?

1. Klanvriendelijkheid/uitstraling

2. Reputatieschade bij fouten

3. Klanten/partners die weglopen

4. Betrouwbaarheid gegevens en gegevensanalyse

5. Sancties: administratieve geldboeten kunnen oplopen tot 20 000 000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

WAAR HET OM GAAT IS DEZE ALGEMENE REGELS TE VERTALEN NAAR DE PRAKTIJK

AVG Routeplanner

- **Projectplan**
- **Dat inventarisatie**
- **Risicoanalyse**
- **Gegevensbeschermingseffectbeoordeling**
- **Organisatieinrichting**
- **Contacten met en verantwoordelijkheid voor derden**
- **Interne Communicatie**
- **Verwerkersovereenkomst**
- **Privacybeleid**
- **Datalekprotocol**
- **Individuele rechten**
- **Privacycontroleur**