A De AVG in een Notendop

Deze appendix is voornamelijk bedoeld voor degenen die het gedeelte over de AVG in hoofdstuk 4 zo boeiend vonden dat ze er meer over willen weten. Daarom heb ik met deze appendix wat extra informatie toegevoegd, gratis en voor niks! Mocht je daar echter totaal geen interesse in hebben, dan kun je hem gerust overslaan.

Voordat de AVG in werking trad kon ieder Europees land zelf hun privacywetgeving invullen met een eigen wet. Dat kwam door de Europese *Richtlijn 95/46/EG* uit 1995. Daar is in Nederland de Wet Bescherming Persoonsgegevens (WBP) uit voortgevloeid, die van 2001 tot 2016 geldig was. Deze was echter verouderd en sloot niet goed meer aan op de digitale wereld zoals we die nu kennen. Omdat ieder land ook een eigen privacywet had, leverde dit bij bedrijven die internationale handel deden (en dus ook regelmatig persoonsgegevens uitwisselden) veel praktische problemen op. Het kwam wel eens voor dat bepaalde wetten elkaar tegenspraken. Daarom is er gekozen voor harmonie binnen de Europese Unie. De AVG is geen richtlijn, maar een *verordening* en is dus rechtstreeks geldig in alle EU landen. Een verordening laat weinig ruimte over voor eigen invulling vergeleken met een richtlijn. Dit maakt ook internationale informatie-uitwisseling een stuk gemakkelijker, omdat overal dezelfde regels gelden. Het beetje ruimte dat de AVG nog wel voor eigen interpretatie overlaat is in Nederland concreet gemaakt met de *Uitvoeringswet Algemene Verordening Gegevensbescherming* (UAVG).

Privacy by design

Privacy by design houdt in dat organisaties niet lukraak je gegevens mogen verwerken en na een paar jaar plotseling kunnen denken: goh, was er niet zoiets als een privacywet? Misschien moeten we daar iets mee doen. *Nein*! Een organisatie is verplicht om van tevoren al goed na te denken over hoe ze gaan zorgen dat je privacy geborgd wordt en dat je persoonsgegevens volgens de wet verwerkt worden. Dat moet dus al in de 'ontwerpfase', vandaar de naam Privacy by design.

Privacy by default

Standaard moeten instellingen privacy-vriendelijk zijn. Een organisatie moet standaardinstellingen (*default settings*) toepassen die alleen persoonsgegevens verwerken die ze nodig hebben om het doel te bereiken dat ze van tevoren hebben opgesteld. Denk aan die extra vinkjes die ze niet van tevoren al mogen zetten, maar ook dat apps niet meer gegevens verzamelen dan ze strikt nodig hebben. In artikel 25 van de AVG staat letterlijk:

> *" […] dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt."*[1]

Bijvoorbeeld: bij het aanmaken van een Facebook-account moet dit zo ingesteld staan dat alles wat jij post alleen zichtbaar is voor jou. Je kunt dit aanpassen, maar dan is die verandering wel blijvend tot je het weer terug zet. In de eerste instantie mag Facebook (of welke organisatie dan ook) niet die keuze voor jou al gemaakt hebben. In de Nederlandse AVG tekst heet dit 'Gegevensbescherming door standaardinstellingen'.

Natuurlijk persoon vs. rechtspersoon

Persoonsgegevens gaan over een *natuurlijk persoon.* Een natuurlijk persoon is een mens van vlees en bloed met rechten en plichten. Juridisch gezien ben je geen natuurlijk persoon meer als je overlijdt. Ook verlies je dan een aantal rechten, zoals je informationele privacy. Oftewel: Persoonsgegevens over jou zijn na je overlijden geen persoonsgegevens meer.

Een rechtspersoon is een entiteit of organisatie die juridisch gezien zelfstandig deel kan nemen aan rechtsverkeer. Er wordt onderscheid gemaakt tussen publiekrechtelijke rechtspersonen en privaatrechtelijke rechtspersonen. De Staat, de provincies, waterschappen en gemeenten zijn voorbeelden van Publiekrechtelijke rechtspersonen.

Voorbeelden van privaatrechtelijke rechtspersonen zijn besloten vennootschappen (bv's), naamloze vennootschappen (nv's), stichtingen, coöperaties en verenigingen. Als je bijvoorbeeld een gemeente aanklaagt, dan klaag je niet iemand persoonlijk aan (een natuurlijk persoon dus), maar de gemeente als publiekrechtelijke rechtspersoon.

Er zijn meerdere verschillen tussen natuurlijke personen en rechtspersonen. Een natuurlijk persoon kan trouwen, een rechtspersoon niet. Een rechtspersoon kan daarentegen wel *fuseren* met een andere rechtspersoon. Een natuurlijk persoon kan overlijden, een rechtspersoon kan ontbonden worden. Een natuurlijk persoon kan een gevangenisstraf krijgen en een rechtspersoon niet, maar een rechtspersoon kan wel een boete krijgen.

Meer over persoonsgegevens

Je heb als het goed is al gelezen dat persoonsgegevens gegevens zijn die betrekking hebben op een geïdentificeerde of een identificeerbare natuurlijk persoon. Hieronder even wat voorbeelden zodat duidelijk is wat wel onder persoonsgegevens valt en wat niet. Soms ligt het aan de context.

Jouw voornaam alleen is geen direct persoonsgegeven. Waarom niet? Omdat er wel meer mensen zijn die Charlotte heten. Of Nina. Of Sjakie. Je snapt het wel. Als jij op straat een briefje vindt met de naam 'Billy' erop geschreven, dan is het onmogelijk om de juiste Billy te vinden. Daar heb je toch echt wat meer informatie voor nodig. De naam Billy kan ook een kast zijn van Ikea, dat weet je niet. Daarom is alleen 'Billy' een *indirect* persoonsgegeven, omdat je meer informatie nodig hebt om het te kunnen koppelen aan één specifiek iemand.

Een *volledige naam* is vaak een persoonsgegeven, maar kan ook een indirect persoonsgegeven zijn. De naam *Jan de Vries* komt wel vaker voor in Nederland en om de juiste Jan de Vries te vinden heb je extra informatie nodig, zoals een adres. Echter, de naam Marie-Rebecca van de Hopsieflopsiepoekiewoekoek zou wel een persoonsgegeven zijn, want die is uniek. Ik heb die naam trouwens zelf verzonnen. Valt niet op, toch?

Een beschrijving van iemand kan zelfs een persoonsgegeven zijn, als iemand daar mee geïdentificeerd kan worden. Die beschrijving moet dan wel specifiek genoeg zijn. Als ik praat over 'de huidige president van Amerika', dan weet iedereen dat ik het over Joe Biden heb. Zodra ik begin te roddelen over 'de actrice die Black Widow speelt', dan weet iedereen dat het over Scarlett Johansson gaat.

Je hebt ook biometrische persoonsgegevens. Denk aan je pasfoto of je vingerafdruk. Ook een irisscan, retinascan en zelfs een afgietsel van je oorschelp gelden als biometrische persoonsgegevens.

Je mobiele telefoonnummer is gekoppeld aan een contract en dat contract staat op naam van één persoon. Daarom is je mobiele nummer ook een (indirect) persoonsgegeven. Het kenteken van je auto is ook een indirect persoonsgegeven, want ergens is een database waar dat kenteken aan je naam en adres is gekoppeld. Anders zouden al die verkeersboetes nooit op de goede deurmat vallen en dat zou vervelend zijn.

Het getal 41 op zich is geen persoonsgegeven. Als je echter onder behandeling bent bij een podotherapeut en speciale schoenen nodig hebt vanwege een medische reden, dan is jouw schoenmaat 41 als onderdeel van een medisch dossier weer wél een persoonsgegeven.

Bedrijfsgegevens zijn per definitie geen persoonsgegevens. Dat betekent dat bijvoorbeeld financiële gegevens van een bedrijf niet onder de AVG vallen. Voor het verwerken van dat soort gegevens zijn voor organisaties dan weer wel andere regels, standaarden of wetten.

De zes grondslagen

Organisaties die persoonsgegevens verwerken mogen dat alleen doen als ze daar een wettelijke grondslag voor hebben, anders is de verwerking niet rechtmatig. Ik heb de zes grondslagen al genoemd, maar hier zijn ze nogmaals met wat meer uitleg.

1. **De organisatie heeft *toestemming* van de betrokkene** Als jij formeel toestemming geeft aan een organisatie om je persoonsgegevens te verwerken, dan mag die organisatie dat doen. Je hebt de voorwaarden voor toestemming kunnen lezen in hoofdstuk 4.
2. **Het verwerken is noodzakelijk om een *overeenkomst* uit te voeren** Als je bijvoorbeeld een abonnement neemt bij een aanbieder van mobiele telefonie, dan is het logisch dat zij bepaalde gegevens van jou nodig hebben, zoals je volledige naam en je bankrekeningnummer. Die provider verwerkt dan je persoonsgegevens.
3. **Het is *wettelijk verplicht* om persoonsgegevens te verwerken** Als jij een baan hebt is je werkgever bijvoorbeeld verplicht om een kopie van je legitimatie in een dossier te bewaren, dat staat in de Wet op de Identificatieplicht. Het bewaren van een kopie van je legitimatie valt onder verwerken. Ook kan de politie je bevelen om bepaalde persoonsgegevens te verstrekken voor een strafrechtelijk onderzoek.

4 **Het is noodzakelijk om persoonsgegevens te verwerken om iemands *vitale belangen* te *beschermen*** Als er acuut gevaar dreigt voor iemands gezondheid en diegene niet in staat is om toestemming te verlenen mag je diens gegevens verwerken. Stel, je loopt langs het huis van je buurman en je ziet hem flauwvallen in zijn woonkamer. Je mag dan zijn naam en adres aan de ambulancedienst geven. Toestemming vragen is in zo'n geval niet nodig. De ambulancedienst maakt dan onderdeel uit van de organisatie die de persoonsgegevens van je buurman verwerkt.
5 **Het is noodzakelijk om persoonsgegevens te verwerken om een *taak van algemeen belang of openbaar gezag* uit te voeren** Belangrijk om te vermelden is dat het hier gaat om wettelijke taken, dus niet iedere organisatie kan zich zomaar beroepen op deze grondslag. Een gemeente kan bijvoorbeeld camera's ophangen ter bevordering van de openbare veiligheid, maar dat mag alleen als minder ingrijpende middelen niet effectief genoeg gebleken zijn. Camera's registreren biometrische persoonsgegevens, omdat mensen herkenbaar in beeld staan.
6 **Een organisatie kan het noodzakelijk vinden om persoonsgegeven te verwerken om een *gerechtvaardigd belang* te behartigen** Dit hoeft geen wettelijke taak te zijn, maar moet wel goed doordacht zijn. Je mag als organisatie niet zomaar inbreuk maken op iemands privacy. Door deze grondslag te gebruiken zeg je eigenlijk: "Het belang van de organisatie is in dit geval belangrijker dan de privacy van de persoon van wie we persoonsgegevens willen verwerken." Bijvoorbeeld: je wilt grensoverschrijdend gedrag op de werkvloer laten onderzoeken en beëindigen. Het kan zijn dat je dan iemands e-mailaccount moet doorspitten naar bewijsmateriaal. De inbreuk op iemands privacy kan dan behoorlijk fors zijn, maar er zijn dus gevallen waarbij je dat zou mogen. Hier zijn geen vaste regels voor, maar wel richtlijnen. In principe mogen alle organisaties deze grondslag gebruiken wanneer ze dat nodig vinden en kunnen verantwoorden, met één uitzondering: overheidsinstanties. De overheid zal dus één van de andere grondslagen moeten gebruiken bij het verwerken van persoonsgegevens. Meestal zal dat een wettelijke verplichting zijn.

Politie en justitie

De AVG geldt niet voor politie en justitie bij het uitvoeren van taken voor het opsporen en vervolgen van strafbare feiten. Ook bij het uitvoeren van straffen geldt de AVG niet. Daarvoor is de *Richtlijn gegevensbescherming politie & justitie*. Vanuit die richtlijn zijn de *Wet politiegegevens* (Wpg) en de *Wet justitiële en strafvorderlijke gegevens* (Wjsg) opgesteld.

Omdat deze wetten niet onder de AVG vallen zijn er dus andere regels. Politie en justitie hebben speciale bevoegdheden nodig om hun taken goed uit te kunnen voeren. Omdat ze wel vaak heel gevoelige gegevens verwerken moeten zij extra goed letten op de beveiliging van die gegevens. Een buitengewoon opsporingsambtenaar (boa) die persoonsgegevens verwerkt voor zijn/haar opsporingstaak valt ook onder de Wpg en niet onder de AVG.

Strafrechtelijke gegevens worden ook wel eens gerekend als negende categorie bijzondere persoonsgegevens. Dat is logisch, omdat strafrechtelijke gegevens ook heel gevoelig zijn. Voor strafrechtelijke gegevens zijn er maar twee uitzonderingen op het verbod op verwerking. De eerste is dat het verwerken onder toezicht moet staan van de overheid. De tweede is dat het verwerken van die gegevens toegestaan is bij een nationaal recht.

Functionaris Gegevensbescherming

Een Functionaris Gegevensbescherming (FG) is binnen een organisatie op het hoogste niveau verantwoordelijk voor het toezien op het toepassen en naleven van de AVG. De Engelse benaming is Data Protection Officer (DPO). Niet alle organisaties zijn verplicht een FG aan te stellen. De organisaties die dat wel verplicht zijn:

- overheidsinstanties en publieke organisaties;
- organisaties die vanuit hun primaire activiteiten op grote schaal mensen en hun activiteiten volgen en/of in kaart brengen;
- organisaties die vanuit hun primaire activiteiten op grote schaal *bijzondere persoonsgegevens* verwerken;
- organisaties die *strafrechtelijke gegevens* verwerken.

Een organisatie die het niet verplicht is kan er alsnog voor kiezen om vrijwillig een FG aan te wijzen, maar dan moet die zich wel aan dezelfde regels houden als een verplichte FG.

Data Protection Impact Assessment

Het kan zijn dat een organisatie verplicht is om een Data Protection Impact Assessment (DPIA) uit te voeren. Dat moet de organisatie dan doen vóórdat ze persoonsgegevens gaan verwerken. Een DPIA uitvoeren betekent dat je als organisatie onderzoekt wat eventuele privacyrisico's kunnen zijn bij het verwerken van persoonsgegevens. Denk dan aan de risico's van diefstal, datalekken enzovoort. Nadat die risico's in kaart gebracht zijn moet de organisatie natuurlijk ook maatregelen nemen om die risico's zo klein mogelijk te maken. Een DPIA maken is niet iets éénmaligs; organisaties zijn altijd in bewe-

ging, waardoor risico's ook weer kunnen veranderen. Als er (grote) veranderingen plaatsvinden moet er ook weer een nieuwe DPIA worden gemaakt.

Meer over bijzondere persoonsgegevens

Hier onder nogmaals de lijst met categorieën. Bijzondere persoonsgegevens hebben betrekking op iemands:

- ras of etniciteit;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- lidmaatschap van een vakvereniging/vakbond;
- gezondheid (medische gegevens);
- seksueel gedrag/seksuele gerichtheid;
- genetische gegevens;
- biometrische gegevens, als deze zijn bedoeld om iemand te identificeren.

Medische gegevens gaan over jou, maar genetische gegevens kunnen ook gaan over andere mensen in je familie; daarom vallen genetische gegevens in een aparte categorie. Als jij een erfelijke ziekte hebt zegt dat iets over jou, maar wellicht ook over je ouders en misschien over je kinderen. Een monster van je dna valt dus onder genetische persoonsgegevens.

Biometrische gegevens gaan over lichamelijke kenmerken of gedragskenmerken. Niet alle biometrische persoonsgegevens vallen onder bijzondere persoonsgegevens. Het gaat alleen om biometrische gegevens die gebruikt worden om iemand te identificeren, zoals de pasfoto op je paspoort. De pasfoto van mijn vrouw die ik in m'n portemonnee heb is wel een persoonsgegeven, maar géén bijzonder persoonsgegeven. Ik gebruik die foto immers niet om haar te identificeren, maar omdat ik van haar houd (en omdat zij een foto van mij in haar portemonnee heeft, dus ja, dan moet je wel…).

Je rechten als datasubject

Als een organisatie jouw persoonsgegevens verwerkt, ben jij het 'datasubject'. Ik licht hier alle rechten nog even kort toe.

Recht op inzage & rectificatie

Als datasubject heb je het recht om te zien welke persoonsgegevens een organisatie over jou verwerkt. In de meeste gevallen moet een organisatie gehoor geven aan je verzoek. Ze zijn in ieder geval verplicht om eerst je identiteit te controleren en dat is natuurlijk om jouw eigen privacy te beschermen; niemand anders moet zomaar inzage kunnen krijgen in jouw persoons-

gegevens. Een organisatie moet je binnen een maand een kopie aanleveren, tenzij je verzoek heel ingewikkeld is. Dan mogen ze er drie maanden over doen, maar dan moeten ze je wel binnen één maand laten weten waarom dat zo is.

In hoofdstuk 4 vertelde ik dat een organisatie geen geld mag vragen als je je persoonsgegevens wil inzien. Als je echter meerdere kopieën opvraagt mogen ze dat wél, maar dat moet een 'redelijke' vergoeding zijn. Het kan ook zijn dat je verzoek wordt geweigerd, maar dat mag een organisatie niet zomaar doen. Als je bijvoorbeeld erg veel verzoeken indient bij dezelfde organisatie kunnen ze besluiten te weigeren. Ook kan een organisatie je verzoek weigeren als jouw verzoek zou leiden tot extreem hoge administratiekosten of als de privacy van andere personen zou worden geschonden. Dan is het ook nog mogelijk dat een organisatie je verzoek weigert om de openbare veiligheid te bewaren of om strafbare feiten te voorkomen of op te sporen. Als een organisatie een verzoek van je weigert, zijn ze in ieder geval verplicht je te laten weten *waarom* ze dat doen. Een organisatie kan ook gedeeltelijk inzage weigeren, door bijvoorbeeld delen uit een dossier weg te halen die de privacy van anderen kan schenden. Je krijgt dan alleen de informatie te zien die betrekking heeft op jouzelf en niemand anders.

Recht op vergetelheid

Er zijn gevallen dat je beroep kunt doen op het recht op vergetelheid. Dat betekent dat een organisatie jouw gegevens moet 'vergeten', oftewel verwijderen uit hun systeem. Er kunnen verschillende redenen zijn om beroep te doen op dit recht:

1. De organisatie heeft hun doel bereikt met de gegevens en heeft de gegevens niet meer nodig.
2. Er is sprake geweest van de grondslag *toestemming* en je hebt die toestemming weer ingetrokken.
3. Je maakt een bezwaar tegen het verwerken van je gegevens.
4. Er worden gegevens onrechtmatig (dus zonder geldige grondslag) verwerkt.
5. Er is sprake van een wettelijke bewaartermijn, maar die is verlopen.
6. Er is sprake van gegevensverwerking via een app of website van iemand die jonger is dan 16 jaar.

N.B.: als je succesvol beroep doet op het recht op vergetelheid, dan moet de organisatie ook al hun back-ups van je persoonsgegevens verwijderen.

Recht op dataportabiliteit

Dataportabiliteit betekent dat je persoonsgegevens overdraagbaar moeten zijn naar een andere organisatie. Een bekend voorbeeld hiervan is je televisie- en internetabonnement. Vertrek je bij een provider? Dan heb je het recht om je persoonsgegevens te ontvangen zodat je deze gemakkelijk aan je nieuwe provider kunt geven. Je kunt ook vragen om je persoonsgegevens rechtstreeks over te laten dragen naar een nieuwe provider. De provider waar je weggaat is verplicht hier aan mee te werken.

N.B.: Alle rechten hebben grenzen. Dataportabiliteit geldt alleen voor digitale gegevens. Papieren dossiers vallen niet onder dit recht. Ook gaat het alleen om gegevens die met de grondslag *toestemming* of een *overeenkomst* verwerkt zijn. Gegevens die volgens andere grondslagen worden verwerkt tellen niet mee.

Recht op beperking van verwerking

Als je de indruk hebt dat een organisatie onjuiste persoonsgegevens verwerkt, dan kun je dat aangeven. De beste manier is schriftelijk. Die organisatie moet dan eerst controleren of de persoonsgegevens correct zijn voordat ze verder mogen gaan met verwerken. Denk je dat je persoonsgegevens onrechtmatig worden verwerkt, maar wil je die later nog wel kunnen opvragen? Dan kun je ook beroep doen op dit recht. Het kan zijn dat een organisatie persoonsgegevens van jou (heeft) verwerkt en haar doel daarmee heeft bereikt. Dan moeten ze die gegevens wegdoen, maar als jij die gegevens nog nodig hebt voor bijvoorbeeld een juridische procedure, dan kun je beroep doen op dit recht om te zorgen dat de gegevens nog wel bewaard worden maar niet verder worden verwerkt.

Als je een bezwaar indient tegen de verwerking van gegevens moet een organisatie stoppen met verwerken. Vervolgens moet die organisatie uitzoeken of zij een gerechtvaardigde grondslag hebben voor het verwerken van die gegevens. Het kan daarbij nodig zijn om uit te zoeken of het belang van de organisatie zwaarder weegt dan jouw belang. Totdat dit uitgezocht is mogen ze die gegevens niet verwerken.

Recht op een menselijke blik bij besluiten

Een andere naam voor dit recht is het *Recht met betrekking tot geautomatiseerde besluitvorming en profilering.* Je kunt tegenwoordig bijvoorbeeld online een lening afsluiten. Je vult wat gegevens in en vervolgens zie je of je die lening krijgt of niet. Zo'n proces is vaak volledig geautomatiseerd. Stel dat je wordt afgewezen voor zo'n lening, dan kun je je beroepen op dit recht.

Dan moet je aanvraag nog een keer in behandeling worden genomen, maar dan door een persoon in plaats van een computer. Dat wil dus *niet* meteen zeggen dat je zo'n lening wel krijgt als je beroep doet op dit recht. Het betekent alleen dat het genomen besluit in ieder geval door mensenogen bekeken moet worden om te kijken of je aanvraag terecht is afgewezen of niet. De aanvraag kan vervolgens alsnog afgewezen worden. Die automatische besluitvorming kan komen doordat de organisatie aan profilering doet. Dan maken ze het besluit op basis van een profiel van jou. Op basis van je profiel kan een organisatie bepaalde inschattingen maken. Dat profiel houdt dus in dat ze je in één of meerdere groepen categoriseren om je gedrag te voorspellen.

Organisaties die aan geautomatiseerde besluitvorming en profilering doen, zijn verplicht om dat in hun privacyverklaring te melden. Heb je de indruk dat dit jou overkomen is, lees dan voordat je een klacht indient eerst die verklaring. Ook kun je aan een besluit zelf vaak zien dat het automatisch is gegenereerd. De tekst is dan heel algemeen en vaak wordt het ook vermeld. Als jij vraagt een organisatie een besluit te herzien moeten ze dat in de meeste gevallen binnen één maand doen. Uitzondering is als je situatie erg ingewikkeld is, dan mogen ze er totaal drie maanden over doen. Ze moeten dat dan wel binnen die eerste maand laten weten. Ze mogen hier geen geld voor vragen, maar ze zijn wel verplicht om jou te identificeren. Dat is voor je eigen privacy natuurlijk, zodat iemand anders niet zomaar jouw gegevens kan inzien.

Recht om bezwaar te maken tegen gegevensverwerking

Je kunt altijd bezwaar maken tegen het verwerken van je persoonsgegevens, maar of daar gehoor aan gegeven moet worden ligt aan de situatie. De Autoriteit Persoonsgegevens noemt twee gevallen waarin mensen zich kunnen beroepen op het recht op bezwaar. De eerste situatie is als een organisatie je gegevens gebruikt voor directe marketing. Er zijn gevallen dat een organisatie je ongevraagd reclamepost mag sturen. Bijvoorbeeld: als je al een bestaande klant bent en producten hebt gekocht die vergelijkbaar zijn met de producten in de reclame. Maak je echter bezwaar, dan moeten ze direct stoppen met die reclame sturen.

De tweede reden om beroep te kunnen doen op dit recht heeft te maken met jouw persoonlijke situatie. Je kunt bij twee grondslagen bezwaar maken en daarbij een specifieke reden benoemen waarom je niet wilt dat je gegevens verwerkt worden. Die grondslagen zijn 1) een taak van algemeen belang of 2) een taak van gerechtvaardigd belang. Er moet dan wel uitgezocht worden wiens belangen hogerop staat, want een organisatie mag alleen door-

gaan met de verwerking als ze kunnen aantonen dat hun belangen zwaarder wegen dan die van jou. Totdat dit duidelijk is mag de organisatie je gegevens niet verwerken.

Recht op informatie

Je hebt recht op duidelijke informatie. Een organisatie is verplicht jou goed te informeren welke informatie ze over je verwerken en met welk doel. Die informatie moet je ook terug kunnen vinden in de privacyverklaring. Dit betekent dus ook dat jij al geïnformeerd moet zijn vóórdat je persoonsgegevens worden verwerkt. Je kunt er (net zoals velen) voor kiezen om de privacyverklaring niet te lezen. Als je toestemming geeft en vervolgens beroep doet op dit recht, dan kan het zijn dat je wordt verwezen naar de privacyverklaring. De organisatie moet in die verklaring onder andere vermelden:

- welke grondslag er gebruikt wordt voor het verwerken van je persoonsgegevens;
- welke persoonsgegevens ze verwerken;
- met welk doel ze die gegevens verwerken;
- of ze je gegevens delen of doorverkopen en zo ja, met wie ze dat doen;
- hoe lang ze je gegevens bewaren;
- hoe de organisatie zelf te bereiken is.

> **Let op**
> Geen enkel recht is absoluut, dus er zijn altijd wel uitzonderingen mogelijk waarom je geen beroep kunt doen op een bepaald recht. Op de website van de Autoriteit Persoonsgegevens kun je veel informatie vinden over deze rechten en voor al deze rechten een voorbeeldformulier downloaden om er gebruik van te maken.

De volledige AVG lezen?

Mocht je wat tijd over hebben en behoefte hebben aan een uitdaging, dan kun je via **deze link** de gehele wettekst van de AVG lezen:

Conclusie

De AVG is er om EU-burgers te helpen en te beschermen. De regels kunnen af en toe streng lijken, maar uiteindelijk is dat allemaal voor een goed doel. Ik heb dingen gekozen om toe te lichten waarvan ik vind dat iedereen ze zou moeten weten. Er is nog veel meer te leren over de AVG en als je daar echt meer over wilt weten, sla dan het hoofdstuk over aanbevolen literatuur niet over!