



## UvA-DARE (Digital Academic Repository)

### "Bent u al klaar voor de AVG?"

*De nieuwe gegevensbescherming in de EU*

Barnhoorn, D.

#### Publication date

2018

#### Document Version

Final published version

[Link to publication](#)

#### Citation for published version (APA):

Barnhoorn, D. (null). (2018). "Bent u al klaar voor de AVG?": De nieuwe gegevensbescherming in de EU., EU Explainer. <http://euexplainer.nl/?p=453>

#### General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

#### Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

# EU Explainer



---

*Zin en onzin over de Europese Unie*

Menu 

---

## “Bent u al klaar voor de AVG?” De nieuwe gegevensbescherming in de EU

Dominique Barnhoorn / 26 maart 2018 / EU en de lidstaten, Grondrechten en Rechtsstaat



Dezer dagen worden organisaties overstelpt met de bovenstaande vraag door advocaten- en consultancykantoren. Privacyjuristen lopen zich warm: op 25 mei treedt de [Algemene Verordening Gegevensbescherming](#) (AVG) namelijk in werking. Dit bijzondere stukje

Europese wetgeving kan verstrekkende gevolgen hebben voor alle organisaties die persoonsgegevens verwerken in Nederland; dat kunnen naast alle grote bedrijven ook zzp'ers, mkb'ers en natuurlijke personen zijn. Vanaf 25 mei 2018 zijn zij namelijk verantwoordelijk voor het – volgens eisen die het Europees recht stelt aan databescherming – correct opslaan en verwerken van hun klantbestanden. Dit artikel bespreekt de meest relevante punten uit de verordening, waaronder hetgeen *wat* je kan doen als consument zodra je recht op bescherming van persoonsgegevens wordt geschonden. Daarmee duikt ook de vraag op: is de consument zelf eigenlijk al klaar voor de AVG? Met het nieuws rond Facebook en Cambridge Analytics afgelopen week nog vers in het geheugen, is die vraag relevanter dan ooit.

### *In het kort...*

De algemene verordening gegevensbescherming werd twee jaar geleden – in april 2016 – door het Europees Parlement goedgekeurd vanuit de behoefte aan nieuwe wetgeving die de Europese burger moest beschermen tegen bedrijven die willekeurig en zonder waarborgen de kostbare klantgegevens verwerkten voor allerhande diensten en services. De oude databeschermingsrichtlijn uit 1995 kon de technologische ontwikkelingen op de [Europese interne markt](#) niet meer bijbenen en daarmee de gegevensbescherming van klantgegevens niet waarborgen. Op Europees niveau werd daarom gekeken naar een verordening die zowel de verdergaande economische integratie kon begeleiden als effectievere bescherming van persoonsgegevens kon bieden aan EU burgers. Dat werd na lange en moeilijke onderhandelingen uiteindelijk de AVG.

### *Gevolgen voor organisaties*

Met de AVG komen er twee zeer belangrijke veranderingen voor organisaties die persoonsgegevens verwerken. Ten eerste kunnen er (zeer) hoge boetes worden opgelegd door de toezichthouder ([Autoriteit Persoonsgegevens](#)) als bijvoorbeeld een bedrijf zich niet houdt aan de databeschermingsregels. Anders dan de oude wetgeving moeten organisaties vanaf 25 mei onder andere kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG te voldoen. Bij schending van deze regels kan de boete oplopen tot 20 miljoen euro óf 4% van de jaaromzet, al naargelang de omstandigheden van het geval. Enkele toetsingscriteria zijn bijvoorbeeld de aard, ernst en duur van de inbreuk, en de opzettelijke of nalatige aard van de inbreuk.

Ten tweede dient een organisatie die grootschalig individuen volgt of persoonsgegevens verwerkt, een functionaris voor gegevensbescherming aan te stellen. Deze persoon controleert of het bedrijf – of andere instantie die gegevens verwerkt – zich houdt aan de

regels voor gegevensbescherming. Daarnaast is de functionaris het contactpunt tussen het bedrijf en de Autoriteit Persoonsgegevens.

### *Is de consument er klaar voor?*

Met het boetebeding in het achterhoofd is er grote kans dat bedrijven al nauwkeurig de ontwikkelingen van de verordening hebben gevolgd. Maar de verordening schetst ook de rechten voor klanten (de ‘betrokkenen’) van bedrijven die persoonsgegevens verwerken. Zo hebben klanten onder andere het recht op transparantie en communicatie (wat doet het bedrijf met mijn gegevens?), het recht om kosteloos informatie en toegang tot eigen persoonsgegevens op te vragen, recht op inzage en rectificatie van persoonsgegevens en, een belangrijke sinds EU Hof van Justitie hierin [uitspraak](#) heeft gedaan, het recht om ook weer vergeten te worden.

Als een organisatie, ondanks een verzoek van een betrokkene, géén van de bovenstaande rechten in acht neemt, kan de betrokkene een klacht indienen bij de AP. Daarnaast is klagen uiteraard mogelijk als het bedrijf sowieso persoonsgegevens op de verkeerde manier verwerkt. De Autoriteit communiceert met de klager over het verdere verloop van de procedure en neemt uiteindelijk een bindend besluit: de organisatie heeft wel of geen inbreuk gemaakt op persoonsgegevens. Wanneer een inbreuk wordt geconstateerd, heeft de klager recht op een schadevergoeding en wordt de organisatie voor de inbreuk aansprakelijk gehouden. Daarnaast kan de Autoriteit Persoonsgegevens nog een extra administratieve geldboete opleggen, afhankelijk van de omstandigheden van het geval. Dit kan, zoals hierboven genoemd, oplopen tot 20 miljoen euro of 4% van de totale jaaromzet.

Het is ook mogelijk om als EU-burger een klacht in te dienen bij de toezichthoudende autoriteit van een andere lidstaat als de inbreuk een grensoverschrijdend karakter heeft. Bijvoorbeeld een sociaal netwerkbedrijf dat persoonsgegevens verwerkt om advertenties te kunnen tonen op basis van het internetgedrag van de bezoekers. De autoriteit van de betreffende lidstaat neemt dan de klacht op en communiceert met de Nederlandse Autoriteit Persoonsgegevens over het verdere verloop van de procedure. Dit wordt ook het “onestopshop” mechanisme genoemd.

### *Wat zijn de verwachtingen?*

Privacy-minnend Nederland wacht af wat er na 25 mei gaat gebeuren. Wordt de Autoriteit Persoonsgegevens overspoeld met klachten van consumenten die een inbreuk constateren, of komen er veel vragen van organisaties die nog niet aan de nieuwe privacyregels voldoen? Daarnaast is het nog onzeker hoe het “onestopshop” mechanisme gaat werken vanwege de

verschillen in nationaal procedurerecht van de 28 EU-lidstaten. Maar het belangrijkste: met deze verordening zet Europa een belangrijke stap in de eenentwintigste eeuw en krijgen ook uw gegevens hopelijk de bescherming die ze verdienen. En u, de consument, heeft een nieuwe optie tot uw beschikking om bedrijven tot de orde te roepen als zij die bescherming niet bieden.

Foto: [Richard Blech](#)

[#AVG](#), [#Databescherming](#), [#Facebook](#), [#Privacy](#)

---

*« Previous / Next »*

---

## Gepubliceerd door **Dominique Barnhoorn**



Dominique Barnhoorn is als PhD-onderzoeker Europees recht verbonden aan het Amsterdam Centre for European Law and Governance (ACELG, UvA) sinds januari 2017. Ze heeft haar mastergraad Europees recht aan de Universiteit Leiden behaald (2015) en daarnaast een master in Rechtsfilosofie (2016, Universiteit Leiden) afgerond. Alle berichten van Dominique Barnhoorn weergeven

---