

Verbeterpunten van de nieuwe privacyverordening

25 januari 2012 [Bits of Freedom](#)

Op 25 januari heeft de Europese Commissie [de nieuwe privacyregels](#) gepresenteerd. De Privacyrichtlijn stamt uit 1995 en was nodig aan modernisering toe. We hebben het pakket kritisch doorgenomen en sommen negen punten op die in ieder geval beter kunnen. We zullen de komende tijd constructieve input geven aan de Europese Commissie om privacy van de internetter beter te beschermen.

- **De boetemaxima moeten hoger.** In een gelekt concept waren de boetemaxima bij overtreding 5% van de wereldwijde omzet. Dat is nu teruggebracht naar 2%. Dat moet hoger: boetes moeten een voldoende afschrikwekkend effect hebben.
- **De opslag van gegevens.** Net als de huidige regels verbieden de nieuwe regels bedrijven om gegevens van gebruikers langer op te slaan dan nodig is. Nieuw is de verplichting om (i) gebruikers te informeren over de duur van de opslag en (ii) om regelmatig na te gaan of de opgeslagen gegevens nog langer gebruikt of bewaard mogen worden, of dat ze niet meer nodig zijn. Wij vinden dat de nieuwe regels een duidelijke verplichting moeten bevatten om gegevens voor een bepaalde vaste periode op te slaan, zonder de mogelijkheid om die bewaartermijn steeds stilzwijgend te verlengen.
- **Dataminimalisatie.** De nieuwe regels verplichten bedrijven en overheden om zo weinig mogelijk persoonsgegevens te verwerken. Een mooi uitgangspunt, maar de verplichting is gerelateerd aan de doelen die bedrijven willen bereiken met het gebruiken van jouw gegevens. Door die doelen stilaan uit te breiden, kan er van het principe van dataminimalisatie in de praktijk weinig overblijven. Wij vinden dat er kritisch gekeken moet worden naar de mogelijkheid om gegevens steeds voor nieuwe doelen aan te wenden en dat deze mogelijkheid tot verdere verwerking beperkt moet worden.
- **Informatieverplichting.** Bedrijven moeten gebruikers informeren over de verwerking van hun gegevens, en dat moet in duidelijke en begrijpelijke taal. Die verplichting bestond al, maar in de praktijk moest je paginalange, onleesbare privacy statements doorploegen. Wij vinden dat alle gebruikers recht hebben op echt duidelijke en begrijpelijke informatie. Dit is extra belangrijk als het gaat om gegevens van internetters, omdat de verwerkingen van online gegevens vaak complex en ondoorzichtig zijn.
- **Dataportabiliteit.** Nieuw is het recht van gebruikers om een kopie te krijgen van elektronisch opgeslagen gegevens, en het recht om deze gegevens van het ene naar het andere bedrijf te verplaatsen. Dat maakt wisselen van sociaal netwerk in theorie een stuk eenvoudiger. Dit recht wordt echter beperkt door de voorwaarde dat gegevens moeten zijn opgeslagen in een 'commonly used format'. Wij vinden dat gebruikers recht hebben op hun elektronisch opgeslagen gegevens, in welk format die ook zijn opgeslagen, en dat gebruikers die moeten kunnen importeren in een ander netwerk.
- **The right to be forgotten.** Er is al veel te doen geweest om het nieuwe 'right to be forgotten'. Dit recht van gebruikers op verwijdering van hun online gegevens leek in de conceptversie van de nieuwe regels nogal wat ruimte te bieden voor geschiedsherschrijving. Het uiteindelijke 'recht op vergetelheid' is een stuk genuanceerder en werkbaarder. Wij vinden dat dit recht actief onder de aandacht van gebruikers moet worden gebracht, inclusief het recht om van een bedrijf te eisen dat zijn derde partijen die je gegevens hebben ontvangen, te informeren over jouw verzoek om verwijdering.
- **Grondslagen voor verwerking.** Net als onder de huidige regels zijn er zes grondslagen waarop bedrijven gegevens mogen verwerken. In de praktijk worden nu veel verwerkingen van je gegevens gebaseerd op een vaag begrip: het

'gerechtvaardigd belang' van bedrijven. Wij moeten ervoor waken dat de afweging tussen de gerechtvaardigde commerciële belangen van bedrijven en jouw recht op privacy niet doorslaat naar bedrijven. Bedrijven moeten deze uitzondering niet kunnen gebruiken om de toestemmingseis te omzeilen.

- **Meldplicht datalekken.** De nieuwe regels bevatten ook een brede meldplicht datalekken. Een datalek moet binnen 24 uur gemeld worden aan de toezichthouder, en ook individuele gebruikers moeten op de hoogte worden gesteld van een lek als het waarschijnlijk is dat het lek een nadelig effect zal hebben op de privacy van gebruikers. Wij zijn blij met deze brede meldplicht datalekken, maar betreuren het dat de regels niet voorzien in een centraal openbaar register van datalekken. Dit kan nog worden verbeterd.
- **One-stop-shop.** Voor internationale bedrijven is het goed nieuws dat ze onder deze nieuwe regels nog maar met één toezichthouder te maken krijgen, in plaats van in ieder EU land met een andere autoriteit te maken krijgen. Een dergelijke 'one stop-shop benadering heeft als nadeel dat bedrijven mogelijk kiezen voor contact met de toezichthouder die het minst streng is, en contact met de striktere toezichthouders bewust vermijden. Wij vinden dat het 'one stop shop principe' niet mag leiden tot 'rondshoppen' van bedrijven naar een lakse toezichthouder.
- **Bescherming tegen buitenlandse mogendheden.** De privacyregels zijn ook bedoeld om te voorkomen dat buitenlandse mogendheden zomaar informatie van Europeanen opvragen. Maar dat wordt vrijwel niet geregeld en wordt later uitgewerkt. Dat moet veel beter: die bescherming moet niet worden overgelaten aan lagere regelgeving maar helder in de Verordening worden uitgewerkt.

Er zijn ongetwijfeld nog meer punten die beter kunnen. Laat ze horen in de comments.