Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

M +31 (0)6 1795 3655
E janneke.sloetjes@bof.nl
W www.bof.nl

Leden van de Commissie Veiligheid en Justitie

Betreft
Reactie Bits of Freedom inzake de conceptverordening gegevensbescherming

Datum
Amsterdam, 2 maart 2012

Geacht lid van de Commissie Veiligheid en Justitie,

1. Op 7 maart overlegt 2012 de Tweede Kamer met de minister van Veiligheid en Justitie over de ontwerpverordening gegevensbescherming (de "**verordening**"). Omdat de verordening gevolgen heeft voor de privacy van internetgebruikers delen wij graag onze gedachten hierover. De verordening is een goed uitgangspunt, maar moet naar de mening van Bits of Freedom worden aangescherpt, onder meer op de volgende punten:

    - De verordening moet bescherming bieden tegen opvraging van persoonsgegevens door buitenlandse autoriteiten en tegen het gebruik door nationale overheden.
    - De definitie van het begrip persoonsgegeven moet ook gegevens waarmee een persoon van anderen kan worden onderscheiden, omvatten.
    - De verordening moet volledig van toepassing zijn op gratis diensten en geen algemene uitzonderingen maken voor bedrijven op basis van hun vestigingsplaats of omvang.
    - De nieuwe rechten voor betrokkenen moeten zó worden uitgewerkt dat ze internetgebruikers daadwerkelijk bescherming bieden en geen loze letter worden.
    - De meldplicht datalekken moet breder worden geformuleerd en worden uitgebreid met een centraal meldingenregister.
    - De bevoegdheden van toezichthouders moeten duidelijker worden geformuleerd en de voorgestelde onderlinge controle van toezichthouders moet kritisch worden bekeken.
    - De grote rol van de Europese Commissie bij de handhaving van de verordening en de vaststelling van regelgeving moet kritisch worden beoordeeld.
    - De verordening moet geen algemene uitzondering bevatten voor gebruik van persoonsgegevens door overheden en aansluiten bij internationale regels.
    - De e-Privacyrichtlijn moet ondergeschikt worden gemaakt aan de verordening en de verhouding tussen de instrumenten moet worden verduidelijkt.

2. Dat lichten we hieronder toe.

Behandeling parlement belangrijk moment om privacy van Nederlanders te beschermen

3. In Nederland wordt de bescherming van persoonsgegevens nu geregeld in de Wet bescherming persoonsgegevens (“Wbp”). Die wet is gebaseerd op de Privacyrichtlijn (Richtlijn 95/46/EC). De bedoeling van de Europese Commissie is dat deze richtlijn wordt vervangen door een verordening. Een verordening heeft rechtstreekse werking en hoeft dus niet in nationale wetgeving geïmplementeerd te worden. De regels gaan over de bescherming van persoonsgegevens van alle Europeanen en gelden de private sector en voor een groot deel van de publieke sector (de Commissie heeft ook een voorstel gedaan voor een nieuwe richtlijn die de de verwerking in het kader van de opsporing en vervolging van strafbare feiten zou regelen).

4. De Europese Commissie heeft een concept voor de verordening op 25 januari 2012 gepresenteerd. De verordening zal naar verwachting de komende twee jaar wordt vastgesteld in Brussel. De regering zal het Nederlandse standpunt uitdragen in de Raad van Ministers, waarna de Raad een gemeenschappelijk standpunt bepaalt.

5. Door het geplaatste behandelvoorbehoud kan de Tweede Kamer invloed uitoefenen op de inbreng van de regering en zo zorg voor de bescherming van de persoonsgegevens van Nederlandse en Europese burgers. De bespreking in de Tweede Kamer is dus een belangrijk moment om de toekomst van privacy in Nederland te bepalen.

Uitgangspunt verordening is goed, maar kan op belangrijke punten beter

6. De ontwerpverordening is honderden pagina's lang en regelt talloze complexe terreinen. Ons commentaar is noodzakelijkerwijs beperkt van aard. Dat gezegd hebbende, vormt de verordening naar de mening van Bits of Freedom in algemene zin een vooruitgang ten opzichte van de huidige regels. De verhoging van de boetes op overtredingen en het mechanisme voor consistente handhaving in alle Lidstaten is een verbetering, net zoals de verduidelijking van het begrip 'toestemming' en de invoering van een aantal nieuwe artikelen die tot doel hebben internetgebruikers beter te beschermen. Op deze punten moet de bescherming die de verordening biedt, niet worden afgezwakt. Wij zien echter ook ruimte voor verbetering en aanscherping van een flink aantal onderdelen van de verordening. Dit wordt hierna per onderwerp toegelicht.

7. Bits of Freedom benadrukt dat haar commentaar zich beperkt tot de verordening, en dat wij niet ingaan op de ontwerprichtlijn die ziet op de verwerking van persoonsgegevens in het kader van de opsporing.

Doorgifte data aan overheden moet met waarborgen worden omkleed

8. Eén van de belangrijkste gebreken in de verordening is dat ze geen regels geeft over het verstrekken van persoonsgegevens door de private sector aan overheidsdiensten, bijvoorbeeld in het kader van de opsporing. Verantwoordelijken moeten dus zelf besluiten in welke gevallen ze persoonsgegevens verstrekken, en dat leidt tot rechtsonzekerheid en ongelijkheid in de behandeling van persoonsgegevens van burgers.

9. Ook zijn er geen regels opgenomen over de internationale doorgifte van persoonsgegevens naar aanleiding van een verzoek van een buitenlandse rechtbank of autoriteit. Deze doorgifte kan onder de voorgestelde verordening plaatsvinden zonder dat een rechtshulpverdrag bestaat tussen de Lidstaat en de verzoekende staat, en zonder dat voorafgaande toestemming van een toezichthouder is vereist. Daardoor is het onvermijdelijk dat buitenlandse regelgeving inbreuk zal maken op het Europese recht op bescherming van persoonsgegevens.

> **Advies** De verordening moet strikte regels stellen met betrekking tot de verstrekking van persoonsgegevens door private partijen aan Europese overheidsinstellingen. Ook moet er bescherming worden geboden tegen buitenlandse opvragingen van persoonsgegevens van Europese burgers.

Persoonsgegevens zouden ook individualiserende gegevens moeten omvatten

10. De verordening gaat bij de definitie van het begrip 'persoonsgegeven' uit van *identificeerbaarheid*, oftewel het verbinden van een naam aan een persoon. Gebruikers kunnen op basis van unieke nummers en (online) gedrag echter steeds vaker *geïndividualiseerd* (onderscheiden van de rest) worden zonder dat ze ook worden *geïdentificeerd*. Ook individualisering kan er toe leiden dat personen in het maatschappelijk verkeer anders worden beoordeeld. Het begrip 'persoonsgegeven' moet daarom worden uitgebreid en ook gegevens omvatten waarmee een individu kan worden *onderscheiden* van anderen.

> **Advies** De verordening moet worden aangepast zodat gegevens waarmee een persoon van anderen kan worden *onderscheiden* ook worden beschouwd als persoonsgegevens.

Toepassing verordening op kleine en buitenlandse bedrijven moet worden gegarandeerd

11. De aanknopingspunten voor toepasselijkheid van de verordening kunnen ook worden verbeterd. Zo is de verordening nu slechts van toepassing op verantwoordelijken (bedrijven of overheden) die goederen en diensten aanbieden in de Europese Unie (“**EU**”) of die het gedrag van Europeanen monitoren. De verordening moet echter expliciet ook van toepassing wordt verklaard op verantwoordelijken die gratis diensten aanbieden, omdat veel internetdiensten die grote

hoeveelheden persoonsgegevens verwerken gratis aan het publiek aangeboden.

12. De verordening stelt tegelijkertijd middelgrote en kleine bedrijven met minder dan 250 werknemers vrij van bepaalde verplichtingen. Ook hoeven bedrijven met minder dan 250 werknemers die buiten de Europese Unie gevestigd zijn geen vertegenwoordiger in de EU aan te wijzen voor de naleving van de verordening. Dit geldt ook voor bedrijven (ongeacht hun omvang) die gevestigd zijn in een land dat een 'adequaat beschermingsniveau' biedt.

13. Die beperkingen zijn onterecht. Het is niet logisch of verstandig om de mate van bescherming van persoonsgegevens van burgers af te laten hangen van de omvang of locatie van een bedrijf. Ook bedrijven met een klein aantal medewerkers kunnen grote hoeveelheden persoonsgegevens verwerken en risicovolle verwerkingen uitvoeren. Door het ontbreken van een vertegenwoordiger in de EU wordt het handhaven van de verordening jegens die bedrijven bovendien tijdrovend en moeilijk. Tot slot garandeert een 'adequaat beschermingsniveau' in de praktijk helaas maar weinig bescherming: er wordt maar een keer vastgesteld dat een land een 'adequaat beschermingsniveau' heeft, en die controle wordt vervolgens nauwelijks meer herzien. Het ligt daarom meer voor de hand om eventuele uitzonderingen op de toepasselijkheid van de verordening te relateren aan de omvang van de verwerking van persoonsgegevens.

> **Advies** De verordening moet volledig van toepassing worden op gratis diensten. Er moeten geen algemene uitzonderingen worden gemaakt voor kleine bedrijven of bedrijven die gevestigd zijn in bepaalde landen.

Rechten van betrokkenen moeten worden versterkt

14. De verordening introduceert het concept *privacy by design*: al in de ontwerpfase moet rekening worden gehouden met de privacybelangen van eindgebruikers. Daarnaast bepaalt het nieuw opgenomen principe van *privacy by default* dat de standaardinstellingen van diensten zo restrictief mogelijk moeten zijn. Samen met het in de verordening opgenomen principe van *data minimisation,* op basis waarvan verantwoordelijken niet méér persoonsgegevens mogen verwerken dan ze nodig hebben voor het bereiken van hun doelen, kunnen deze artikelen er in theorie voor zorgen dat internetgebruikers online beter de regie over hun persoonsgegevens kunnen voeren. Bits of Freedom omarmt deze beginselen dan ook. In de praktijk moeten deze regels wel effectief worden geïmplementeerd om er voor te zorgen dat ze daadwerkelijk de bescherming bieden die ze beloven. Het is belangrijk dat het parlement hier goed op toeziet.

15. De verordening introduceert ook het recht op *data portability*: gebruikers krijgen het recht op een elektronische kopie van hun persoonsgegevens en mogen hun gegevens exporteren naar een andere verantwoordelijke (bijvoorbeeld van Hyves naar Facebook), maar alleen als de verantwoordelijke de gegevens in een 'algemeen gebruikt' format verwerkt. Dit artikel moet worden uitgebreid met een aanpassingsverplichting zodat gebruikers hun persoonsgegevens

kunnen ontvangen, onafhankelijk van het format waarin de verantwoordelijke de gegevens verwerkt.

16. Ook het nieuw geïntroduceerde *right to be forgotten* moet verder worden uitgewerkt. Het artikel maakt nog niet duidelijk wanneer gegevens van een betrokkene verwijderd moeten worden wanneer de betrokkene zelf gegevens heeft verstrekt, of wanneer een derde deze gegevens heeft gepubliceerd. In de praktijk kan het *right to be forgotten* ook conflicteren met het recht op informatievrijheid. Conflicten tussen het recht op privacy en het recht op informatievrijheid zullen moeten worden opgelost aan de hand van de ontwikkelde jurisprudentie van het EHRM.

17. Tot slot moet het toestemmingsvereiste worden verduidelijkt, zodat onomstotelijk komt vast te staan dat toestemming nooit gegeven kan worden door middel van (aanpassingen van) algemene voorwaarden.

> **Advies** Rechten van betrokkenen moeten zo geïmplementeerd worden dat er geen uitholling plaatsvindt. De afweging met andere fundamentele rechten moet daarnaast zorgvuldig worden gemaakt.

Uitgangspunt voor datalekken moet worden aangepast, meldpunt geïntroduceerd

18. De verordening bevat de verplichting voor verantwoordelijken om de toezichthouder én betrokkene op de hoogte te brengen van een datalek waarbij persoonsgegevens van betrokkenen bijvoorbeeld op straat komen te liggen: een 'meldplicht datalekken'. Deze meldplicht is nog niet voldoende uitgewerkt en beschermt betrokkenen in onvoldoende mate. In de eerste plaats omdat de meldplicht gekoppeld is aan het begrip 'personal data breach', en dus uitgaat van een inbreuk op beveiligingsmaatregelen.

19. Naar de mening van Bits of Freedom zou niet de *inbreuk op beveiligingsmaatregelen*, maar de *ongeautoriseerde toegang tot persoonsgegevens* leidend moeten zijn. Het verlies van persoonsgegevens kan zich immers ook voordoen *zonder* dat er inbreuk wordt gemaakt op beveiligingsmaatregelen, bijvoorbeeld omdat iemand per ongeluk een database met vertrouwelijke gegevens op internet plaatst zonder die te beveiligen. Ten tweede ontbreekt een centraal openbaar meldpunt datalekken. Zo'n centraal openbaar meldpunt geeft betrokkenen de mogelijkheid om een goed overwogen keuze te maken ten aanzien van de aan wie zij hun data willen toevertrouwen en zal bedrijven en overheden stimuleren om hun beveiliging zo goed mogelijk in te richten.

> **Advies** De meldplicht moet uitgaan van onbevoegde toegang tot persoonsgegevens en er moet een openbaar meldpunt worden geïntroduceerd.

Handhaving binnen Europa moet worden gestroomlijnd

20. De handhaving van de verordening is in handen van de nationale toezichthouders (“**DPA's**”). Ondernemingen met meerdere vestigingen in de Europese Unie kunnen straks terecht bij één toezichthouder, de 'lead DPA'.

21. Dit *one-stop shop* principe kan afbreuk doen aan de bescherming van de rechten van betrokkenen. Ten eerste biedt de tekst van de verordening ondernemingen nog te veel ruimte om verantwoording af te leggen aan de DPA die het minst goed zal handhaven. Ten tweede kunnen DPA's in bepaalde Lidstaten door het *one-stop shop* principe overbelast raken. Zowel Facebook, Google als Microsoft zijn bijvoorbeeld in Ierland gevestigd, wat voor grote druk op de Ierse DPA zal zorgen. Een groot deel van de DPA's kampt nu al met gebrek aan capaciteit en technische kennis.

22. De verordening stelt DPA's in staat om controle uit te oefenen op een “*lead DPA*”. Wanneer een burger in Duitsland een klacht over Facebook indient bij de Duitse DPA, zal de Ierse DPA de *lead DPA* zijn. De Duitse DPA heeft dan het recht om de werkwijze van de Ierse DPA controleren. Het is maar zeer de vraag of de Duitse DPA dat echt zal doen omdat dat zowel omslachtig als politiek complex is. Deze werkwijze verzwakt dus uiteindelijk de positie van de Europese en in het bijzonder de Duitse burger.

> **Advies** De verordening moet duidelijker aangeven welke DPA bevoegd is. Capaciteiten van DPA's moeten worden aangepast waar nodig en de werkwijze en onderlinge controle van DPA's moet kritisch worden bekeken.

Rol van de Europese Commissie moet kritisch worden bekeken

23. De Europese Commissie zal toezicht houden op de handhaving van de verordening door nationale DPA's. DPA's moeten maatregelen aan de Europese Commissie voorleggen. De Commissie kan vervolgens besluiten om over te gaan tot schorsing. Ook heeft de Commissie het recht om implementatiewetten op te stellen waarin de juiste uitleg van de verordening wordt bepaald. Ook bevat de verordening op een groot aantal onderdelen verwijzingen naar gedelegeerde maatregelen en uitvoeringshandelingen. Dat soort maatregelen en handelingen worden door de Europese Commissie vastgesteld zonder dat een actieve rol van het Europees Parlement vereist is. De rol van de Europese Commissie bij de handhaving van de verordening wordt daarmee enorm groot, bijvoorbeeld op het gebied van het vaststellen van regels over de internationale doorgifte van persoonsgegevens.

> **Advies** Er moet kritisch gekeken worden naar de rol van de Europese Commissie. Het Europees Parlement moet meer inspraak krijgen bij de

uitwerking en vaststelling van regelgeving op verschillende onderwerpen, zoals internationale doorgifte.

Regelgeving moet minder versnipperd en verwijzen naar internationale regels

24. De verordening geldt in beginsel zowel voor private partijen als voor de overheid, met uitzondering van verwerking van persoonsgegevens in het kader van de opsporing en vervolging van strafbare feiten. Daarop is ontwerprichtlijn (COM 2012/10) van toepassing, die tegelijkertijd met de verordening door de Commissie is voorgesteld.

25. Ook *binnen* de verordening wordt echter al onderscheid gemaakt tussen verplichtingen van private partijen en van overheden. In combinatie met de hierboven genoemde ontwerprichtlijn ontstaat er zo een versnipperd geheel aan regelgeving, in plaats van een allesomvattend kader dat de rechten en verplichtingen van gebruikers in alle omstandigheden duidelijk maakt.

26. Tegelijkertijd verwijst de verordening niet naar het Dataprotectieverdrag van de Raad van Europa (Conventie 108). Dat is een gemis, omdat deze conventie het enige verdrag over gegevensbescherming is met een wereldwijde reikwijdte. Een verwijzing naar het verdrag maakt duidelijk dat deze verordening tot doel heeft de regels neergelegd in Conventie te respecteren en daarbij aan te sluiten.

Advies De verordening moet geen algemene uitzonderingen bevatten voor gebruik van persoonsgegevens door overheden en aansluiten bij internationale regelgeving met betrekking tot bescherming van persoonsgegevens.

De verhouding met e-Privacy Richtlijn moet worden verduidelijkt

27. De verordening bepaalt dat de e-Privacyrichtlijn (Richtlijn 2002/58/EC) ongewijzigd blijft gelden. Dat zal leiden tot tegenstellingen en versnippering van regelgeving op het gebied van bescherming van persoonsgegevens. De Europese Commissie moet daarom vaststellen dat de ePrivacy Richtlijn ondergeschikt wordt aan de verordening, en in een mededeling de verhouding tussen de verordening en de richtlijn uiteenzetten.

Advies De verhouding tussen de e-Privacy Richtlijn en de verordening moet worden verduidelijkt.

28. Bits of Freedom vertrouwt er op dat deze brief de Tweede Kamer handvatten biedt om op 7 maart met de minister in overleg te treden over de verordening. Wij zijn vanzelfsprekend graag

bereid om de bovenstaande opmerkingen verder toe te lichten wanneer daar behoefte aan bestaat.

Hoogachtend,

Janneke Slöetjes