

Datum: 7 januari 2026

Nominaties Big Brother Awards 2025

Bits of Freedom



INLEIDING

De prijs voor de grootste privacyschenders van Nederland, de Big Brother Awards, is een initiatief van Bits of Freedom. Bits of Freedom selecteerde de vijf grofste schandalen van het afgelopen jaar. Het publiek kan, door te stemmen, bepalen welke genomineerde de Publieksprijs mee naar huis neemt en een vakjury zal de winnaar van de Expertprijs bepalen. Bits of Freedom reikt daarnaast ook de positieve Felipe Rodriguez Award uit, aan een persoon die een buitengewone bijdrage heeft geleverd aan het beschermen van onze digitale rechten. De uitreiking vindt plaats tijdens een awardceremonie op 20 februari 2026 in Vlaams Cultuurhuis de Brakke Grond te Amsterdam.

INHOUDSOPGAVE

INLEIDING	2
INHOUDSOPGAVE	3
1. NOMINATIE: BELASTINGDIENST	4
2. NOMINATIE: CLINICAL DIAGNOSTICS NEDERLAND	6
3. NOMINATIE: MICROSOFT	8
4. NOMINATIE: NATIONALE POLITIE	10
5. NOMINATIE: VERENIGING VAN NEDERLANDSE GEMEENTEN	12
6. VERANTWOORDING	14

1. NOMINATIE: BELASTINGDIENST

De Belastingdienst is genomineerd voor het onrechtmatig inzetten van algoritmen.

WAT IS ER GEBEURD?

De Belastingdienst zet zo'n honderd algoritmen in, waarbij in veel gevallen gebruik wordt gemaakt van risicoprofilering.¹ Op basis van persoonlijke kenmerken, zoals leeftijd, woonplaats en fiscale geschiedenis, wordt er bepaald of je een risicogeval bent. Van de zo'n honderd algoritmen die worden ingezet, blijkt de helft niet aan de wettelijke regels te voldoen.² Het gaat op meerdere vlakken mis: de Belastingdienst verzaakt haar wettelijke plicht om bij risicovolle verwerkingen, waaronder bij de inzet van algoritmen, van te voren in kaart te brengen welke risico's de verwerking met zich meebrengt en welke maatregelen worden genomen om die te mitigeren. Ook houdt de Belastingdienst zich niet aan de plicht om verwerkingen van persoonsgegevens te verantwoorden en te documenteren. Dat zorgt ervoor dat de algoritmen en de uitkomsten niet controleerbaar zijn en er een risico bestaat voor discriminatie. Daarnaast is er niet altijd sprake van menselijke tussenkomst. De Belastingdienst houdt zich dus nog altijd niet aan de wet, met alle risico's van dien.

WAAROM IS DAT ERG?

De Belastingdienst heeft nog niet zo lang geleden een enorme ravage aangericht. Door het toeslagenschandaal zijn tienduizenden gezinnen gedupeerd geraakt door onrechtmatig en oneerlijk handelen. Mensen werden op grote schaal gediscrimineerd. Dit kwam door bewuste keuzes die binnen de organisatie werden gemaakt en door het gebruik van algoritmen. Mensen zijn in enorme schulden terecht gekomen doordat ze onterecht toeslagen moesten terugbetalen. Kinderen zijn uit huis geplaatst en vele slachtoffers zijn jarenlang onder veel stress gebukt gegaan.³ De hersteloperatie is nog niet afgerond en nu blijkt dat de Belastingdienst zichzelf alweer boven de wet plaatst. Ze zet opnieuw algoritmen in, zonder zich iets aan te trekken van wettelijke waarborgen die bestaan om ravages te voorkomen.

Burgers lopen ernstige risico's door de algoritmen die door de Belastingdienst worden ingezet, want de kans bestaat dat de algoritmen discrimineren. Het toeslagenschandaal heeft duidelijk laten zien hoe groot de impact is van discriminerend handelen van de Belastingdienst. Daarnaast bestaat het risico dat de besluiten van de Belastingdienst, die met behulp van de algoritmen gemaakt zijn of zelfs volledig

¹Follow The Money: [Meer dan 50 algoritmes van de Belastingdienst zijn illegaal, zegt de Autoriteit Persoonsgegevens](#) (11 oktober 2025).

²Autoriteit Persoonsgegevens: [Brief Belastingdienst geautomatiseerde selectie-instrumenten](#) (8 augustus 2025).

³Parool: [Kabinet biedt kinderen die na toeslagenaffaire uit huis zijn geplaatst excuses aan en belooft extra steun](#) (30 juni 2025).

automatisch tot stand zijn gekomen, onrechtmatig zijn genomen. Dat zou gevolgen hebben voor alles wat er na het besluit gebeurt, zoals de ontvangen of juist niet ontvangen toeslagen, aanslagen, enzovoorts. Het risico om toeslagen mis te lopen of te moeten terugbetalen ligt bij de burgers. Kortom, doordat de Belastingdienst zich nog altijd niet aan de (privacy)wet houdt, is er opnieuw een enorme puinhoop veroorzaakt waar burgers voor opdraaien.

BITS OF FREEDOM ADVISEERT

De Belastingdienst moet zich onmiddellijk aan de wet gaan houden, waaronder aan de Algemene Verordening Gegevensbescherming. De Belastingdienst moet leren van haar fouten in plaats van dezelfde fouten in veelvoud opnieuw te maken. Daarbij moet ze inzetten op herstel van vertrouwen, in plaats van steeds opnieuw aan te tonen waarom ze het vertrouwen van burgers niet verdient. De Autoriteit Persoonsgegevens moet ophouden zich te gedragen als consultant en daadwerkelijk toezicht gaan houden.⁴ De Belastingdienst moet niet vriendelijk verzocht worden een plan van aanpak op te stellen, maar moet bestraft worden als ze zich niet aan de wet houdt.

⁴Bits of Freedom: [Hoe de Autoriteit Persoonsgegevens consultant van de Belastingdienst werd](#) (30 oktober 2025).

2. NOMINATIE: CLINICAL DIAGNOSTICS NEDERLAND

Clinical Diagnostics Nederland is genomineerd voor het verzwijgen van haar datalek van de gegevens van mensen die deelnamen aan het bevolkingsonderzoek baarmoederhalskanker.

WAT IS ER GEBEURD?

Clinical Diagnostics Nederland, hierna Clinical Diagnostics, is een laboratorium dat onder andere de baarmoederhalskankertest verwerkt voor Bevolkingsonderzoek Nederland. Hiervoor verwerkt zij gevoelige gegevens. Bij het verwerken van dergelijke gegevens komt een grote verantwoordelijkheid kijken. Clinical Diagnostics ontloep die verantwoordelijkheid.

Criminelen verschaften zichzelf toegang tot de gegevens van bijna een miljoen mensen die mee hebben gedaan aan het bevolkingsonderzoek.⁵ Het gaat om naam, adres en woonplaats, geslacht, soort onderzoek (zelftest of uitstrijkje), geboortedatum, BSN-nummer, testuitslag(en) en de naam van de huisarts. Voor sommigen getroffen en geldt dat ook het telefoonnummer en e-mailadres is gestolen. Daarnaast bleek later dat, naast gegevens van het bevolkingsonderzoek baarmoederhalskanker, ook gegevens van huid-, urine- en penisonderzoek waren buitgemaakt.⁶ Een deel van de gegevens is op het darkweb geplaatst. Uit analyse van RTL, van een op het darkweb geplaatste set gegevens, blijkt dat dit gaat om gegevens van 53.516 mensen die bij de huisarts een onderzoek hebben laten doen.⁷ Volgens het Bevolkingsonderzoek is het onduidelijk welk deel precies op het darkweb is gepubliceerd en dus wiens gegevens dit wel/niet betreft.⁸

Bij een datalek is het belangrijk om de getroffen en zo snel mogelijk op de hoogte te stellen en te informeren over welke gegevens zijn gelekt. Daarom geldt de wettelijke verplichting dit binnen 72 uur te melden. In plaats van deze verantwoordelijkheid te nemen verzweeg Clinical Diagnostics de hack bijna een maand lang voor Bevolkingsonderzoek Nederland.⁹ Hierdoor konden de mensen om wiens gegevens het gaat pas een maand nadat het gebeurd was worden geïnformeerd.

Niet alleen richting Bevolkingsonderzoek Nederland is Clinical Diagnostics te traag in haar communicatie. Richting huisartsen wiens patiënten betrokken zijn bij het datalek, duurde het verzwijgen nog langer. Pas in de tweede helft van november, zo'n 4,5 maand na het lek, ontvingen de huisartsen een brief van het laboratorium.¹⁰

⁵Bevolkingsonderzoek Nederland, 'Update datalek bevolkingsonderzoek baarmoederhalskanker' (12 september 2025).

⁶RTL Nieuws, 'Datahack medische wereld blijkt veel groter: ook onderzoek huid, urine en penis gestolen' (11 augustus 2025)

⁷RTL Nieuws, 'Datahack medische wereld blijkt veel groter: ook onderzoek huid, urine en penis gestolen' (11 augustus 2025)

⁸Bevolkingsonderzoek Nederland, 'Veelgestelde vragen datalek' (laatst gezien 24 november 2025).

⁹NOS, 'Bevolkingsonderzoek Nederland: 'Schokkend dat datalek pas na maand bekend werd' (12 augustus 2025).

¹⁰Clinical Diagnostics, 'Update: Donderdag 20 november 2025' (20 november 2025).

WAAROM IS DAT ERG?

Organisaties die met medische gegevens werken, hebben een extra zware verantwoordelijkheid om secuur om te gaan met de gegevensverwerking en de verplichtingen die daarbij horen. Clinical Diagnostics heeft hier duidelijk steken laten vallen. Het laboratorium had Bevolkingsonderzoek Nederland en huisartsen direct op de hoogte moeten stellen, maar heeft in plaats daarvan een tijd over het datalek gezwegen. Daardoor konden Bevolkingsonderzoek Nederland en huisartsen de getroffen personen niet informeren. Hierdoor zijn zij onnodig kwetsbaar gemaakt voor de gevolgen van een datalek, zoals bijvoorbeeld phishing.

Een nadelig effect van nalatig handelen op het gebied van gegevensbeveiliging door medische instellingen zoals Clinical Diagnostics is dat het afbreuk doet aan het vertrouwen in dergelijke instellingen. Dat zorgt vervolgens voor extra hoge drempels om mee te doen aan dit soort onderzoeken, die belangrijk zijn voor de gezondheid van mensen.

BITS OF FREEDOM ADVISEERT

Wees realistisch en eerlijk. Mensen hebben niets aan beloften dat het veilig is of dat het niet weer zal gebeuren, want dat is niet te garanderen. Wel is het belangrijk om zo goed mogelijk met gegevens om te gaan. Dat betekent dat Clinical Diagnostics haar datahuishouding op orde moet hebben, inclusief een plan voor hoe te handelen in het geval van een datalek, die voldoet aan de plicht dit binnen 72 uur te melden. Zolang dit niet op orde is, moet het laboratorium het verwerken van medische gegevens opschorten.

En waarom beschikt dit laboratorium eigenlijk over zoveel gegevens? Een belangrijke waarborg in het beveiligen van gegevens is dataminimalisatie. Immers, over wat je niet hebt kun je ook de controle niet kwijtraken. Bits of Freedom adviseert dat er in het zorgdomein breed wordt gekeken of alle wettelijke verplichtingen tot gegevensverstrekking wel noodzakelijk zijn. Ook adviseert Bits of Freedom dat zowel op juridisch als op organisatie-niveau het principe van dataminimalisatie wordt toegepast.

Meer info: <https://www.bnr.nl/nieuws/juridisch/10580757/ap-onderzoekt-datadiefstal-bevolkingsonderzoek-waarom-had-lab-zo-veel-gegevens>

3. NOMINATIE: MICROSOFT

Microsoft is genomineerd voor haar bijdrage aan de genocide in Palestina vanuit haar datacentrum in onze achtertuin.

WAT IS ER GEBEURD?

Microsoft blijkt sinds eind 2021 diensten te leveren aan de Israëlische geheime dienst Unit 8200. De ambitie van de geheime dienst was het opslaan en analyseren van een miljoen telefoongesprekken per uur. In juni 2025 zou dat gaan om 11,500 terabytes aan gegevens, omgerekend zo'n 200 miljoen uur aan audio.¹¹

De infrastructuur werd niet alleen gebruikt voor het opslaan van de gegevens, maar ook voor de analyse ervan. Die informatie werd gebruikt voor het bepalen van doelen in Palestina om te bombarderen. Ook werd het systeem gebruikt voor het maken van een analyse van de mensen die zich in de directe omgeving van het doel bevonden. Daarnaast werd de informatie gebruikt om mensen te chanteren, mensen vast te zetten of zelfs, al dan niet achteraf, het doden van mensen te rechtvaardigen.¹²

Na berichtgeving in de media hierover stelde Microsoft in eerste instantie dat er geen aanwijzingen waren dat haar systemen werden gebruikt om mensen in Palestina te volgen of te doden. Dat stond haaks op de innige samenwerking tussen de geheime dienst en het technologiebedrijf. In een intern document wordt de samenwerking beschreven als “daily, top down and bottom up.”¹³ Meer dan een maand later stelde Microsoft dat intern onderzoek uitwees dat “bepaalde onderdelen” van de berichtgeving in de media wel klopte. Microsoft meldde daarop de levering van “bepaalde diensten” aan “een unit binnen” het Israëlische ministerie van Defensie te hebben gestaakt.¹⁴

De link met Nederland? Het datacenter van Microsoft waar deze gegevens werden opgeslagen en verwerkt, staat in Middenmeer, in de kop van de Noord-Holland.

WAAROM IS DAT ERG?

Microsoft draagt met haar dienstverlening bij aan de genocide in Palestina. Genociden zijn handelingen met als doel een nationale, etnische of godsdienstige groep, dan wel een groep die behoort tot een bepaald ras, geheel of gedeeltelijk als zodanig te vernietigen.¹⁵ Het aantal doden van de genocide in Palestina wordt op meer

¹¹+972 Magazine: ‘[Microsoft storing Israeli intelligence trove used to attack Palestinians](#)’, (6 augustus 2025).

¹²+972 Magazine: ‘[Microsoft storing Israeli intelligence trove used to attack Palestinians](#)’, (6 augustus 2025).

¹³The Guardian: ‘[A million calls an hour: Israel relying on Microsoft cloud for expansive surveillance of Palestinians](#)’, (6 augustus 2025).

¹⁴Microsoft: ‘[Update on ongoing Microsoft review](#)’, (25 september 2025).

¹⁵Overheid.nl: ‘[Verdrag inzake de voorkoming en de bestraffing van genocide](#), Parijs’ (geldend vanaf 18 september 1966).

dan 70.000 mensen geschat, het aantal gewonden op meer dan 170.000.¹⁶ ¹⁷ Gaza is onleefbaar geworden en Palestijnen leven in onmenselijke omstandigheden. Israël deed dit bewust, aldus Amnesty International.¹⁸ Microsoft had zich, gezien de intieme samenwerking, bewust moeten zijn van haar rol in deze genocide, en haar verantwoordelijkheid moeten nemen. Dit gaat ver voorbij de vraag of Israël gesteund moet worden in het beschermen van haar belangen.

Daar komt bij dat het datacenter van Microsoft (en ook die van andere technologiebedrijven) toch al controversieel is door het enorme energie- en waterverbruik en het verpesten van het landschap. Microsoft adverteert haar datacenters aan Nederland als een noodzakelijke stap voor geopolitieke onafhankelijkheid en als belangrijke bijdrage aan de werkgelegenheid.¹⁹ Dat maakt het des te pijnlijker dat het datacenter is gebruikt voor het faciliteren van oorlogsmisdaden. En wat betekent de belofte dat “al het personeel van Microsoft in de Wieringermeer drie dagen per jaar vrijwilligerswerk doet bij bijvoorbeeld scholen in de regio” als je het grotere plaatje bekijkt?

In dit licht is het ook onbegrijpelijk hoeveel Nederlandse bedrijven en overheidsinstanties diensten van Microsoft blijven afnemen. Tot zover het maatschappelijk verantwoord ondernemen.

BITS OF FREEDOM ADVISEERT

Bits of Freedom roept Microsoft op om al haar dienstverlening tegen het licht te houden. Het is onbegrijpelijk dat het leveren van technologie aan een geheime dienst van een land dat genocide pleegt, geen alarmbellen heeft doen afgaan. Het is dan ook aannemelijk dat het bedrijf veel vaker diensten levert aan overheden die die dienstverlening inzetten voor het onderdrukken van bevolkingsgroepen.

¹⁶United Nations Office for the Coordination of Humanitarian Affairs (OCHA): ‘[Reported impact snapshot | Gaza Strip](#)’ (30 april 2025).

¹⁷Health Cluster, World Health Organisation: ‘[Palestinian Casualties as reported by the Palestinian Ministry of Health since the 7th of October 2023](#)’ (16 november 2025).

¹⁸Amnesty International Nederland: ‘[Stop de genocide in Gaza](#)’ (5 december 2024).

¹⁹NH Nieuws: ‘[Wéér een datacenter in Middenmeer, Microsoft kondigt uitbreiding aan](#)’ (9 september 2025).

4. NOMINATIE: NATIONALE POLITIE

De Nationale Politie is genomineerd voor het monitoren van activisten via sociale media, en het vervolgens thuis opzoeken van deze activisten, zonder wettelijke grondslag.

WAT IS ER GEBEURD?

De politie heeft, ook dit jaar, met enige regelmaat demonstranten thuis opgezocht. De politie monitort sociale media en maakt registraties van wie er demonstreert of oproept om deel te nemen aan een demonstratie. Vervolgens vraagt de politie de adresgegevens van deze mensen op en belt dan onaangekondigd bij demonstranten thuis aan. Dit gebeurt niet incidenteel. Alleen al onder demonstranten van Extinction Rebellion zijn sinds 2022 maar liefst 35 mensen thuis opgezocht.²⁰

Zelf geeft de politie als reden voor de huisbezoeken dat ze toekomstige demonstraties in goede banen wilt leiden.²¹ Maar de vragen die in de gesprekken worden gesteld gaan helemaal niet over de openbare orde en dragen dus ook niet bij aan de wettelijke taak om demonstraties te faciliteren.²² Integendeel, uit verklaringen van demonstranten blijkt dat de huisbezoeken vooral als doel lijken te hebben om de boodschap af te geven dat ze in de gaten worden gehouden omdat ze naar demonstraties gaan.

Opvallend in dit opzicht is ook dat de politie ervoor kiest om aan te bellen bij ‘gewone’ demonstranten, en niet alleen bij de bekende organisatoren van demonstraties.²³ Voor deze intimiderende vorm van surveillance ontbreekt een wettelijke grondslag en daarmee is het een illegitieme inbreuk op het demonstratierecht en het recht op privacy.

WAAROM IS DAT ERG?

De politie is erg vaag over de functie en status van deze huisbezoeken. Hierdoor weten mensen niet of ze ergens van worden verdacht, of het gesprek telt als een verhoor, wat de aanleiding is voor het huisbezoek, wat er gedaan wordt met wat zij zeggen in het gesprek en wat hun rechten zijn op dat moment. Het gebrek aan bewustzijn van de politie over deze ongelijke machtsverhouding, of de bewuste inzet van deze machtspositie, is stuitend.

²⁰RTV Utrecht: ‘Extinction Rebellion naar rechter na huisbezoek politie aan Amersfoortse demonstrant’ (25 maart 2025).

²¹Follow the Money: ‘Politie zou activisten bezoeken om demonstraties te ondersteunen. Daar klopt niets van’ (4 april 2025).

²²Youtube, Nieuwsplein 33: ‘Demonstrant krijgt huisbezoek Amersfoortse politie. Politie maakt daarna excuses’ (24 maart 2025).

²³Follow the Money: ‘Politie zou activisten bezoeken om demonstraties te ondersteunen. Daar klopt niets van’ (4 april 2025).

Onaangekondigde huisbezoeken aan demonstranten door de politie zijn enorm intimiderend. Er gaat een *chilling effect* van uit. Dat wil zeggen dat het voor mensen veel enger, en dus moeilijker, wordt om deel te nemen aan een demonstratie, ook al willen die mensen dat misschien wel. Een huisbezoek als gevolg van demonstreren geeft een sterk signaal af dat de politie demonstraties afkeurt, en werpt zo onnodige en schadelijke drempels op om democratische rechten, zoals het demonstratierecht en de vrijheid van meningsuiting, uit te oefenen. Immers, je wilt voorkomen dat de politie bij jou aanklopt.

BITS OF FREEDOM ADVISEERT

De politie moet stoppen met intimiderende huisbezoeken van demonstranten. Ze moet werken aan de interne cultuur en het beleid zodat het bij alle individuele agenten duidelijk wordt dat deze bezoeken onacceptabel zijn. De Nationale Politie moet zich richten op haar wettelijke taak om demonstraties te faciliteren en ze moet zich weerhouden van het opwerpen van drempels voor burgers om aan demonstraties deel te nemen.

5. NOMINATIE: VERENIGING VAN NEDERLANDSE GEMEENTEN

De Vereniging van Nederlandse Gemeenten is genomineerd voor het faciliteren van de keuze voor Microsoft.

WAT IS ER GEBEURD?

Afgelopen jaar bleek uit onderzoek dat 62% van de Nederlandse gemeenten op e-mailservers van Microsoft draaien.²⁴ Dat is aanzienlijk meer dan in buurlanden als Duitsland en Frankrijk, waar respectievelijk 4% en 17% van de gemeenten op e-mailservers van Microsoft draaien. In Nederland maken gemeenten veel gebruik van Microsoft, en niet alleen voor e-mailen. In een onderzoek van iBestuur gaven alle van de 54 ondervraagde Nederlandse gemeenten aan gebruik te maken van Microsoft, variërend van Office 365 en Teams tot Azure en Windows.²⁵

Microsoft is een Amerikaans bedrijf en moet zich aan de Amerikaanse wet houden, zoals de Cloud Act, Foreign Intelligence Surveillance Act en bepaalde bevelen van de Amerikaanse president (executive orders). Dat kan uiteenlopende consequenties hebben. Uit de Cloud Act volgt bijvoorbeeld dat, wanneer de Amerikaanse overheid daartoe verzoekt, Microsoft gegevens die in haar bezit zijn moet overdragen aan de Amerikaanse overheid. Daarbij maakt het niet uit waar de server met de gegevens zich fysiek bevindt.²⁶ Nederlandse gemeenten zijn dus door hun afhankelijkheid van Microsoft ook afhankelijk van de Amerikaanse overheid. Dat brengt kwetsbaarheden met zich mee, bijvoorbeeld voor de e-mail van Nederlandse gemeenten. Dat soort communicatie is immers vrijwel nooit end-to-end versleuteld.

De Vereniging van Nederlandse Gemeenten heeft een cloudexpertisecentrum (GGI-Cloud) waar gemeenten terecht kunnen voor hulp bij hun transitie naar de cloud. Daarbij ondersteunt de VNG, in nauwe samenwerking met Microsoft, met allerlei hulpmiddelen de overstap naar de cloud van Microsoft. Ze maakt zelfs prijsafspraken met Microsoft, zodat gemeenten ook de komende jaren weten waar ze op moeten rekenen.²⁷

Dat terwijl slechts enkele gemeenten zich géén zorgen maken over de verplichtingen van Microsoft ten opzichte van de Amerikaanse overheid. Veel gemeenten voelen zich ook 'locked-in': ze voelen zich zodanig afhankelijk van Microsoft dat overstappen niet mogelijk lijkt zonder ernstige gevolgen. Maar 5 van de 54 ondervraagde gemeenten denkt dat een overstap naar een andere leverancier haalbaar is.²⁸ De Vereniging van Nederlandse Gemeenten erkent de risico's en roept op tot

²⁴Jurgen Gaeremyn: 'European critical dependencies' (8 maart 2025).

²⁵iBestuur: 'Gemeenten voelen zich klemgezet door Microsoft' (13 februari 2025).

²⁶Dutch Cloud Community: 'Microsoft geeft toe: de Amerikaanse overheid kan klantdata opeisen' (31 juli 2025).

²⁷Vereniging Nederlandse Gemeenten: 'VNG-aanbestedingskalender' (6 augustus 2025).

²⁸iBestuur: 'Gemeenten voelen zich klemgezet door Microsoft' (13 februari 2025).

een strategische aanpak om digitale autonomie te vergroten, maar wil niet abrupt stoppen met Big Tech.²⁹

WAAROM IS DAT ERG?

De privacy van de inwoners en ambtenaren van gemeenten loopt risico door het grootschalig gebruik van Microsoft, en in het bijzonder door het gebruik van haar e-mailservers. De eerder genoemde Cloud Act, maar ook andere wetgeving, brengt kwetsbaarheden met zich mee, omdat de Amerikaanse overheid Microsoft kan verzoeken om gegevens te overhandigen. In de huidige geopolitieke situatie is dat risico alleen maar nog groter. Gegevens van gemeenten, die ook betrekking kunnen hebben op de inwoners van die gemeenten, zouden vertrouwelijk en beschermd moeten zijn en niet in handen van de Amerikaanse overheid mogen komen.

De Amerikaanse overheid kan bovendien Microsoft dwingen te stoppen met de levering van diensten aan Nederlandse gemeenten. Dat gebeurde eerder al bij het Internationaal Strafhof, waar, op last van Trump, rechters opeens niet meer bij hun e-mail konden.³⁰ Het kan dus zijn dat gemeenten opeens geen gebruik meer kunnen maken van hun digitale infrastructuur. Dat zou grote gevolgen hebben, voor alle gemeentelijke dienstverlening.

De Vereniging van Nederlandse Gemeenten kiest ervoor gemeenten te helpen met hun overstap naar Microsoft, ondanks de risico's die dat met zich meebrengt.

BITS OF FREEDOM ADVISEERT

De Vereniging van Nederlandse Gemeenten moet aansturen op een soevereine, onafhankelijke digitale infrastructuur. Met zo'n infrastructuur zijn gemeenten niet langer afhankelijk van een enkel bedrijf. Ook moet die infrastructuur gebaseerd zijn in Nederland of Europa, waar we meer controle hebben over de wet- en regelgeving voor de bescherming van gegevens en de vertrouwelijkheid van communicatie. De Vereniging van Nederlandse Gemeenten moet vol inzetten op de alternatieven voor de dienstverlening van Microsoft, zodat ook Nederlandse gemeenten weer in vrijheid kunnen opereren.

²⁹iBestuur: 'Gemeenten voelen zich klemgezet door Microsoft' (13 februari 2025).

³⁰EenVandaag: 'Onze afhankelijkheid van Amerikaanse techbedrijven is gevaarlijk in een handelsoorlog: 'Ze kunnen je hele organisatie digitaal uitschakelen' (31 juli 2025).

6. VERANTWOORDING

De vijf genomineerden komen uit een lijst met vele schendingen van onze digitale rechten in het afgelopen jaar. De lijst is gebaseerd op signalen die Bits of Freedom het afgelopen jaar heeft ontvangen. De selectie gebeurde aan de hand van een aantal criteria. De meest doorslaggevende criteria gingen over de mate waarin de schending een inbreuk maakt op de privacy van mensen, het aantal mensen dat geraakt werd, de mate waarin de schending voortduurt, de houding van de schender, de mate waarin de schending met feitelijke informatie onderbouwd kon worden en de mate waarin onze achterban zich zorgen maakt over de schending.

In aanloop naar de prijsuitreiking op vrijdagavond 20 februari 2026 kan het publiek stemmen op de vijf genomineerden en daarmee laten zien wie volgens hen de grootste schender van onze privacy is. Daarnaast reikt Bits of Freedom de Expertprijs uit en een positieve prijs voor voorvechters van onze digitale rechten, de Felipe Rodriguez Award.

**Bits of Freedom komt op voor jouw
vrijheid en privacy op internet.**

Deze grondrechten zijn onmisbaar
voor je ontwikkeling, voor
technologische innovatie en voor
de rechtsstaat. Maar die vrijheid is
niet vanzelfsprekend. Je gegevens
worden opgeslagen en geanalyseerd.
Je internetverkeer wordt afgeknepen
en geblokkeerd.

Bits of Freedom zorgt ervoor dat
jouw internet jouw zaak blijft.

Bits of Freedom
bitsoffreedom.nl
🐦 [@bitsoffreedom](https://twitter.com/bitsoffreedom)
Prinseneiland 97HS
1013 LN Amsterdam

Contactpersoon:
Rejo Zenger
+31 6 3964 2738
rejo@bitsoffreedom.nl

1FBF 7B37 6537 68B1 2532
A4CB 0994 0946 21DB EFD4
(bitsoffreedom.nl/openpgp)

**BITS OF
FREEDOM**
Voor jouw internetvrijheid