



Stichting Privacy First

Jaarverslag 2025

12 juli 2026

1.	Voorwoord	1
2.	Visie en beleid	2
3.	Projecten en evenementen	3
3.1	Nederlandse Privacy Awards & Nationale Privacy Conferentie	3
3.2	Publieksdebatten	5
3.3	Overige activiteiten	6
3.3.1	Stille diplomatie	6
3.3.2	Samenwerkingsverbanden	7
3.3.3	Privacy First als dagelijkse vraagbaak	8
4.	Politieke lobby	10
4.1	Financiële privacy	10
4.2	Medische privacy	12
4.3	Kinderen & privacy	13
4.4	Overige onderwerpen	14
5.	Rechtszaken	16
5.1	Rechtszaak tegen ANPR massa-surveillance	16
5.2	Coalitiezaak tegen Amerikaanse overname van DigiD-leverancier	17
5.3	Overige rechtszaken	19
6.	Claimstichting CUIC	20
7.	Communicatie	21
7.1	Massamedia	21
7.2	Internet	22
8.	Organisatie	22
9.	Financiën	23
10.	Vooruitblik 2026 en verder	25

1. Voorwoord

Voor u ligt het jaarverslag 2025 van Stichting Privacy First. In onze jaarverslagen blikken we traditioneel graag terug, maar ook vooruit. Privacy heeft immers de toekomst.

Privacy First weet met beperkt budget telkens van maatschappelijke meerwaarde te zijn, vooral dankzij slimme samenwerking met andere organisaties, pro bono advocaten en professionele vrijwilligers. Zo zorgde Privacy First in 2025 o.a. voor maatschappelijke bewustwording en media-aandacht voor de risico's van "slimme" deurbellen, zorgwekkende ontwikkelingen bij medische gegevensuitwisseling, kwalijke identificatiepraktijken in de financiële sector, massa-surveillance door anti-witwaswetgeving en de risico's van de Europese digitale identiteit en de digitale euro.

Met de komst van de AVG kreeg Privacy First jaren geleden meer wind in de zeilen, maar op ons werkterrein lijkt het tij inmiddels te zijn gekeerd. Vanuit het bedrijfsleven en de Amerikaanse overheid staat het Europese (en daarmee ook het Nederlandse) privacyrecht in toenemende mate onder druk. Juist in deze tijd van geopolitieke spanningen mogen universele waarden, principes en burgerrechten echter niet verkwanseld worden. De les uit het verleden is simpel: grote, centrale databanken met gevoelige gegevens worden in crisistijd misbruikt. Dus is dit precies de tijd om onze Europese en nationale digitale infrastructuur privacyvriendelijk en soeverein te maken: onafhankelijk van Big Tech en buitenlandse wetgeving. Met de Nederlandse Privacy Awards, onze lobby en rechtszaken draagt Privacy First daar graag een steentje aan bij. Dat kan niet zonder financiële steun van fondsen, sponsors en donateurs. Zou uw organisatie graag sponsor of donateur van Privacy First willen worden? Neem dan contact met ons op!



2. Visie en beleid

Privacy First is in 2008 opgericht als onafhankelijke stichting ter behoud en bevordering van ieders recht op privacy. Privacy is een universeel mensenrecht en de basis van onze democratische rechtsstaat. Als Algemeen Nut Beogende Instelling (ANBI) beschermt en bevordert Privacy First het recht op privacy in het algemeen belang, hetzij voor de gehele bevolking, hetzij voor kwetsbare bevolkingsgroepen. Privacy First hanteert daarbij een brede, principiële oriëntatie op privacy, zowel als basis voor onze vrije, open samenleving als voor ieders vrije individuele ontwikkeling. Naast de persoonlijke levenssfeer omvat het recht op privacy de bescherming van persoonsgegevens, vertrouwelijke communicatie, het huisrecht en het recht op lichamelijke integriteit. Privacy is bovendien een voorwaarde voor de uitoefening van talloze andere fundamentele rechten en vrijheden.

Ons blikveld en onze activiteiten strekken zich van oudsher uit tot zowel het digitale als het analoge domein. Deze werelden raken echter in toenemende mate geïntegreerd en maken de klassieke 'analoge ruimte' steeds kleiner. De ontwikkelingen in het digitale domein gaan razendsnel. Om dit in goede banen te kunnen leiden pleit Privacy First naast goede wetgeving met degelijke privacy-waarborgen al jaren voor *privacy by default* en *privacy by design*: het inbouwen van privacy in technologie. De Europese privacywet AVG heeft ons daarbij wind in de rug gegeven. Tegelijkertijd opereert Privacy First immer in een krachtenveld waardoor ieders privacy continu bedreigd wordt.

Vast beleid van Privacy First is om onze aandacht primair te richten op (dreigende) privacy schendingen die grote groepen mensen tegelijk kunnen treffen. In onze selectie van onderwerpen laten wij ons daarbij leiden door 1) de schaal, 2) de ernst en 3) de impact en gevolgen van een bepaalde schending. Massale, ernstige privacy schendingen worden door Privacy First eerst onderzocht en publiekelijk benoemd. Vervolgens probeert Privacy First de betreffende schending op te heffen door stille diplomatie en politieke lobby, eventueel gevolgd door een publiekscampagne, juridische actie of – als uiterste middel – een rechtszaak. In lijn met deze criteria richt de aandacht van Privacy First zich de komende jaren voornamelijk op massasurveillance, financiële privacy, medische privacy, kinderen & privacy (met name in het onderwijs) en het Internet of Things.

Hieronder lichten wij onze voornaamste activiteiten uit 2025 toe, soms in de context van eerdere ontwikkelingen of met een vooruitblik naar 2026. Voor alle actuele activiteiten van Privacy First verwijzen wij u graag naar onze website.

3. Projecten en evenementen

3.1 Nederlandse Privacy Awards & Nationale Privacy Conferentie

Op 28 januari 2026 organiseerden ECP en Privacy First voor de negende achtereenvolgende keer gezamenlijk onze jaarlijkse Nationale Privacy Conferentie. Dit is al jaren hét jaarlijkse Nederlandse privacy-evenement op de Europese Dag van de Privacy. Ons doel van dit evenement is om samen met het bedrijfsleven, de overheid en wetenschap te bouwen aan een privacyvriendelijke informatiemaatschappij en Nederland te helpen ontwikkelen tot internationaal privacy-gidsland. Op onze vaste congreslocatie (Nieuwspoort in Den Haag) waren opnieuw meer dan tweehonderd professionals aanwezig. Sprekers tijdens het congres waren achtereenvolgens Marjolijn Bonthuis (programmamanager Digitale Veiligheid & Vertrouwen, ECP), Bart Schellekens (Rijksorganisatie voor Ontwikkeling, Digitalisering en Innovatie, ministerie van BZK), Sylvia Huydecoper (directeur Platform Zelfstandige Ondernemers en zelfstandig ICT- en privacyjurist), Monique Verdier (vicevoorzitter Autoriteit Persoonsgegevens), Gerrit-Jan Zwenne (hoogleraar Universiteit Leiden en Open Universiteit, advocaat bij Pels Rijcken), Marianne van den Anker (Ombudsvrouw Rotterdam-Rijnmond), Wilmar Hendriks (Control Privacy, Coördinerend functionaris gegevensbescherming, Zorg en Veiligheidshuis Rotterdam-Rijnmond) en Marlon Domingus (juryvoorzitter Nederlandse Privacy Awards). Dagvoorzitter was presentator Tom Jessen (RTL, BNR).



Uitreiking van de Nederlandse Privacy Awards door juryvoorzitter Marlon Domingus tijdens de Nationale Privacy Conferentie (28 januari 2026, Nieuwspoort, Den Haag)

Als afsluitend onderdeel van de conferentie werden door Privacy First onze jaarlijkse [Nederlandse Privacy Awards](#) uitgereikt. Tijdens de zomer en herfst van 2025 ontving Privacy First diverse hoogwaardige inzendingen voor deze Awards. Na een eerste selectie en pitchronde in Amsterdam had de onafhankelijke vakjury de volgende organisaties genomineerd: Publiosa – Registervanverwerkingen.nl (online publicatie van verwerkingsregisters voor (semi-)overheden), LROI & Bluegen.ai (orthopedische zorgdata voor onderzoek via hoogwaardige synthetische datasets), Stimulansz – Privacy Kwartet (trainingsinterventie voor privacybewustwording bij gemeenten), UMC Utrecht & Roseman Labs – NSK datawerkplaats (*privacy-by-design* samenwerkingstool ter signalering van kindermishandeling met geavanceerde cryptografie), Stichting Keurmerk Ritregistratiesystemen: onafhankelijke certificering die privacy van zakelijke rijders waarborgt), TNO, NFI & SURF – GPT-NL: eerste Nederlandse LLM dat volledig AVG-conform is ontwikkeld, als blauwdruk voor soevereine en verantwoorde AI in Europa).



Tijdens de conferentie hebben alle genomineerden hun projecten met Award-videopitches aan het publiek gepresenteerd.

UMC Utrecht & Roseman Labs, Stichting Keurmerk Ritregistratiesystemen en TNO, NFI & SURF werden vervolgens door de jury tot [winnaars](#) uitgeroepen.

Daarnaast ging de Aanmoedigingsprijs naar het Nationaal innovatie centrum privacy-enhancing technologies (Nicpet).

De jury van de Nederlandse Privacy Awards bestond in 2025 uit de volgende experts:

- Marlon Domingus (juryvoorzitter)
- Walter van Wijk
- Koen Versmissen
- Jaap-Henk Hoepman
- Lora Mourcous
- Sulaika Duijsings-Mahangi
- Sah Farooq
- Jan Rinia.

De uitreiking van de Nederlandse Privacy Awards werd in 2025-2026 mede mogelijk gemaakt door NordVPN. Mediapartner is PONT Data & Privacy. Zie voor meer informatie over de Privacy Awards (inclusief een overzicht van alle winnaars en genomineerden sinds 2018) <https://privacyfirst.nl/privacyawards/>.

Op 28 januari 2027 zullen Privacy First en ECP dit inspirerende evenement opnieuw organiseren. Wil uw organisatie graag partner of sponsor worden? Neem dan contact op met Privacy First!



3.2 Publieksdebatten

Privacy First organiseert regelmatig publieksdebatten over actuele onderwerpen. Op 6 maart 2025 organiseerden we samen met massaclaim-organisatie CUIC een enerverende [publieksbijeenkomst](#) over hoe slachtoffers van privacyschendingen hun recht kunnen halen: *Access to Justice*. Vier sprekers gaven vanuit verschillende invalshoeken presentaties over de bescherming van persoonsgegevens en de juridische strijd tegen privacyschendingen. Na een introductie over CUIC door voorzitter Wilmar Hendriks ging advocaat Jurjen Lemstra in op de stand van zaken bij de massaclaim tegen Avast die CUIC namens gedupeerden is gestart. Daarna ging hoogleraar Gerrit-Jan Zwenne dieper in op het privacyrecht bij massaschadeclaims. Tot slot sprak advocaat Ina Brouwer over de collectieve privacyzaak van slachtoffers van 'bangalijsten'. De debatmiddag stond onder leiding van moderator Frits Huffnagel. Locatie was het Volkshotel in Amsterdam (voormalige kantoorlocatie van Privacy First).

Tevens worden de medewerkers en bestuursleden van Privacy First regelmatig als spreker gevraagd voor andermans publieksevenementen. Zo was onze directeur in 2025 o.a. spreker bij evenementen van de Universiteit Leiden en Lex Digitalis over digitale soevereiniteit.

Richting digitale autonomie: key points

- Huidige wet- en regelgeving vormen geen belemmering om te kiezen voor privacyvriendelijke alternatieven voor Big Tech.
- Idem voor aanbestedingswetgeving? Vooral privacyvriendelijker IT-inkoopbeleid en gunningscriteria nodig, bijv. in relatie tot buitenlandse spionagewetgeving, vereisten van *privacy by design*, open standaarden en *open source*.
- Goed Europees voorbeeld: Duitse deelstaat Sleeswijk-Holstein.
- Kwestie van DOEN en DURVEN KIEZEN!
- Meer onderlinge Europese samenwerking (tussen relevante bedrijven) nodig.
- Investerings vanuit overheid nodig.
- Stapsgewijze omschakeling als weg voorwaarts.

Slide uit presentatie Privacy First tijdens symposium Lex Digitalis over digitale soevereiniteit, 13 november 2025, Koninklijke Schouwburg Den Haag.

Wilt u graag op de hoogte blijven van onze publieksdebatten? Meld u dan via onze website aan voor onze nieuwsbrief!

3.3 Overige activiteiten

Privacy First wordt regelmatig door organisaties, bedrijven en overheden gevraagd om advies. Wanneer de intenties van de betreffende organisatie in lijn liggen met de missie van Privacy First, willen wij graag een bijdrage leveren. Door onze constructief-kritische betrokkenheid tracht Privacy First op deze wijze – in het algemeen belang – bepaalde maatschappelijke ontwikkelingen positief te beïnvloeden en de privacy niet alleen “van buitenaf” maar ook “van binnenuit” te laten waarborgen.

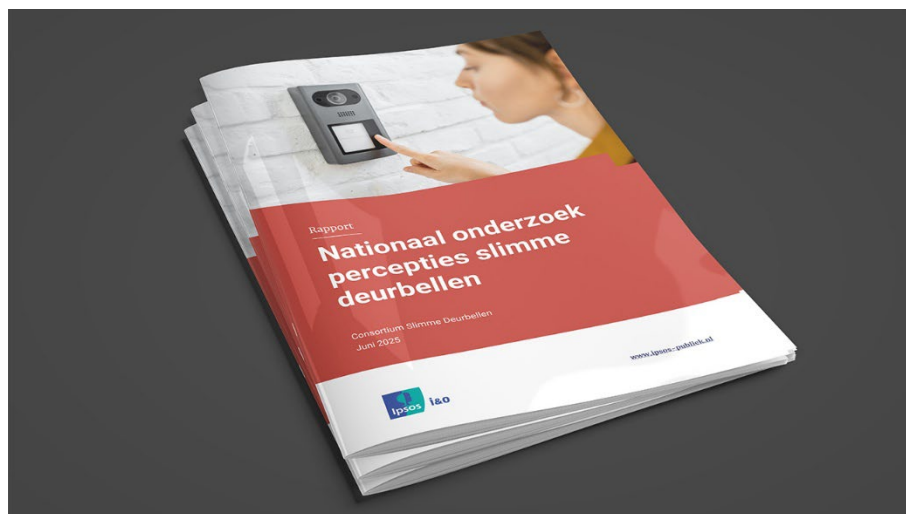
3.3.1 Stille diplomatie

Privacy First voert continu stille diplomatie op ons brede werkkterrein. Mede in dat verband had Privacy First in 2025 (hernieuwde) kennismakingen en meetings met o.a. de Autoriteit Consument & Markt (ACM), Nationale Politie, Autoriteit Persoonsgegevens (AP), Militaire Inlichtingen- en Veiligheidsdienst (MIVD), Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), Nederlands Forensisch Instituut (NFI), Ministerie van Financiën,

Nederlandse Vereniging van Banken (NVB), De Nederlandsche Bank (DNB), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), ECP, Bits of Freedom, Qiy Foundation, Open State Foundation, Public Interest Litigation Project (PILP-NJCM), Verwey-Jonker Instituut, Universiteit van Amsterdam, Wetenschappelijke Raad voor het Regeringsbeleid (WRR), Ministerie van Volksgezondheid, Welzijn en Sport (VWS), Nederlands Normalisatie Instituut (NEN), Rathenau Instituut, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), UNESCO Nederland, Kenniscentrum Filantropie, Stichting Democratie & Media, The Privacy Collective, Rijksdienst voor Identiteitsgegevens (RvIG), Rijksinspectie Digitale Infrastructuur (RDI), ESET Nederland, FBNet, Koninklijke Marechaussee, Nationaal Coördinator tegen Discriminatie en Racisme (NCDR) en BridgeHead.

3.3.2 Samenwerkingsverbanden

“Slimme deurbellen” zijn helaas niet meer weg te denken in Nederland: inmiddels hangen er circa 1,6 miljoen in Nederlandse huishoudens. Deze camera-deurbellen brengen allerlei privacy-, juridische en ontwerp vragen met zich mee. Om die reden is in 2024 het **Slimme Deurbellen Consortium** opgezet; dit is een samenwerkingsverband van het Responsible Sensing Lab, AMS Institute, gemeente Amsterdam, gemeente Groningen, gemeente Den Haag, gemeente Breda, VNG, TU Delft en Privacy First. Het [consortium](#) heeft gedurende 2025 onderzocht hoe deze technologie meer verantwoord kan worden ingezet en welke maatregelen nodig zijn om zowel gebruikers als voorbijgangers te beschermen. Concrete activiteiten van het consortium waren o.a. een [nationaal onderzoek](#) naar percepties over slimme deurbellen (uitgevoerd door Ipsos), gemeentelijke bewustwordingscampagnes, een privacyvriendelijk ontwerp voor een deurbel-lens en juridisch-ethisch onderzoek naar opties voor regelgeving en handhaving. Doel van het consortium is om tevens fabrikanten te gaan beïnvloeden.



Sinds begin 2024 zijn verschillende organisaties een alliantie tegen online seksueel geweld gestart om deze problematiek gezamenlijk aan te pakken. Binnen deze **Boundaries coalitie** bundelen Fonds Slachtofferhulp, Offlimits, het Landelijk Centrum Seksueel Geweld, Fier, Privacy First en Boekx Advocaten hun kennis en expertise. Boundaries zet zich gezamenlijk in voor het ondersteunen van slachtoffers, het vergroten van bewustwording en het bevorderen van preventie van online seksueel misbruik en geweld. Daarnaast doet de alliantie onderzoek, ontwikkelt zij voorstellen richting politiek en toezichthouders of onderneemt zij juridische acties. Afhankelijk van het onderzoek of project werken soms alle partners samen, en soms een deel van de alliantie.

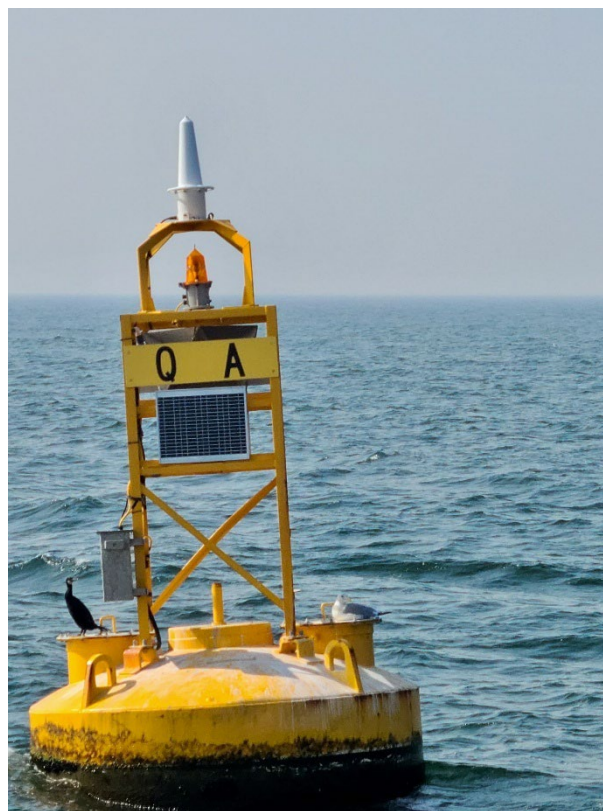


3.3.3 Privacy First als dagelijkse vraagbaak

Naast deze activiteiten wordt Privacy First voortdurend benaderd door burgers met de meest uiteenlopende vragen en verzoeken op privacyterrein. Vooralsnog heeft Privacy First hiervoor helaas nauwelijks capaciteit, dus geven wij mensen vaak kort advies en verwijzen hen door naar andere relevante organisaties, waaronder de AP, Nationale Ombudsman, CTIVD, juristen en advocaten. In 2025 vroegen burgers ons o.a. om hulp bij de volgende kwesties:

- Niet afschermen van medische informatie
- Bewaartermijn surfgegevens en IP-adressen door ISP (Telecommunicatiewet)
- Tv-ploeg filmt zonder toestemming bij organisatie
- Verplichte pas voor milieustraat in gemeente
- Onredelijke eisen LinkedIn om weer toegang te krijgen tot geblokkeerd account
- Surveillance door AIVD
- Vraag om juridische ondersteuning wegens ernstige zorgen over privacy en veiligheid betrokkene

- Advies over AVG-regels omtrent verwerking van gevoelige persoonsgegevens in onbeveiligde Google spreadsheet
- Verplichting van werkgever om een eID-viewer te gebruiken
- Identificatiebeleid Catawiki
- Identiteitsverificatie door banken, verzekeraars en creditcardmaatschappijen
- Mogen patiëntgegevens worden gebruikt voor andere doeleinden?
- Is het legitiem dat een werkgever een kopie van een bankpas maakt?
- Gemaakte fouten door gemeenten
- IT-medewerker kijkt ten onrechte in medische dossiers van zorginstelling
- Zorgen over DigiD dat in Amerikaanse handen zou kunnen vallen
- Passieve opstelling overheid ten aanzien van Big Tech
- Etc. etc.



4. Politieke lobby

4.1 Financiële privacy

Financiële privacy is een belangrijk [aandachtsgebied](#) voor Privacy First, waarbij meespeelt dat andere privacy-organisaties er tot op heden te weinig aandacht voor hebben. Dat geldt niet alleen voor Nederland. In 2025 heeft Privacy First contacten gelegd met relevante Europese organisaties zoals European Digital Rights (EDRI), Finance Watch en Statewatch en daar aandacht gevraagd voor onderwerpen die aandacht verdienen, waaronder riskante identiteitsverificatie door financiële instellingen, de nieuwe Europese regels over bestrijding van criminaliteit door bedrijven (onder andere banken) door middel van grootschalige datagedreven profilering (antiwitwaswetgeving) en de *open banking* voorstellen van de EU.

Riskante identificatie

Het onderwerp identificatie heeft Privacy First aan de orde gesteld in de consultatie van de Europese Banken Autoriteit (EBA), aangezien financiële instellingen er voor burgers riskante identificatiepraktijken op nahouden. (In 2024 vroegen we daar al aandacht voor bij het ministerie van Financiën en DNB). In onze consultatiereactie van juni 2025 heeft Privacy First tevens gewaarschuwd voor het sluipenderwijs verplicht worden van de nieuwe Europese "digitale identiteit", ook wel 'EDI-wallet' of 'EUDI-wallet' genaamd.

In november 2025 namen we deel aan het door het ministerie van BZK georganiseerde Maatschappelijk Overleg Digitale Identiteit en stuurden wij aan het ministerie een groot aantal vragen over het EUDI-wallet systeem.

De schaduwkanten van de privatisering van de criminaliteitsbestrijding

In bovengenoemde EBA-consultatie heeft Privacy First tevens aandacht gevraagd voor de schaduwkanten van de privatisering van de criminaliteitsbestrijding naar bedrijven. Zo leiden die regels onder meer tot grootschalige verspreiding van financiële persoonsgegevens met grote veiligheidsrisico's, wordt geen dataminimalisatie toegepast en vindt discriminatie en uitsluiting plaats.

De Nederlandse regering hield in de zomer van 2025 een consultatie over de uitvoeringsregels van de nieuwe Europese antiwitwaswetgeving. In onze consultatiereactie heeft Privacy First om maatregelen verzocht om de maatschappelijke en persoonlijke schade die door geprivatiseerde misdaadbestrijding ontstaat te mitigeren. Deze consultatiereactie hebben we onder meer onder de aandacht gebracht van AMLA, de nieuwe Europese antiwitwasautoriteit.

Digitale euro en verdwijning contant betalen

In november 2025 waarschuwde Privacy First voor de haast automatische uitrol van de digitale euro zonder dat sprake is van democratische legitimatie. Dit kreeg de nodige aandacht en leidde onder meer tot overleg en betrokkenheid bij DNB. Ook de dreigende verdwijning van contant geld blijven we kritisch volgen en waar mogelijk “counteren”, aangezien dit het enige betaalmiddel is dat maatschappelijke inclusie en privacy waarborgt.

Datahandel, profilering en meer

De handel in financiële persoonsgegevens is tot op heden ongereguleerd. Dat heeft tot gevolg dat een groot aantal datahandelaren financiële persoonsgegevens verkrijgt zonder toestemming van betrokkenen en zonder dat de AVG wordt nageleefd. Privacy First bepleit regulering van datahandel en volgt de ontwikkelingen daaromtrent op de voet. Zo loopt er momenteel een rechtszaak bij het Europees Hof van Justitie over het oogsten van persoonsgegevens ten behoeve van een kredietwaardigheidsbeoordeling.

Datagedreven profilering en het gebruik van *artificial intelligence* heeft eveneens onze aandacht, aangezien dat op grote schaal gebeurt met financiële persoonsgegevens, niet alleen bij kredietwaardigheidsbeoordelingen maar ook in de geprivatiseerde misdaadbestrijding. In april 2025 leverde Privacy First in dit verband commentaar in een consultatie door de Autoriteit Persoonsgegevens over betekenisvolle menselijke tussenkomst.

In lijn met onze eerdere activiteiten rond het UBO-register (lobby en rechtszaken) was Privacy First ook in 2025 actief op nationaal en Europees niveau. Mede door onze lobby werd begin 2025 door de Tweede Kamer bepaald dat als een private partij op grond van “legitiem belang” toegang tot het UBO-register krijgt, de betreffende UBO door de Kamer van Koophandel zal worden geïnformeerd over de inzage en over het doel van die inzage. Verdere activiteiten van Privacy First tegen de dreigende openbaarheid van het UBO-register liggen in het verschiet.



Privacy First blijft ook overige relevante ontwikkelingen kritisch volgen en waar mogelijk beïnvloeden, zoals de *open banking* voorstellen van de EU, internationale uitwisseling van financiële persoonsgegevens tussen overheden (FATCA, CRS, DAC) en EU-plannen om een Europese Tax Data Hub op te zetten.

4.2 Medische privacy

Ontwikkelingen rondom de European Health Data Space (EHDS) leidden in 2025 tot een groei van het speelveld rondom de toegang tot medische gegevens. Daadwerkelijke regie door patiënten kwam in grotere mate haaks te staan op de belangen van partijen die medische gegevens willen gebruiken voor onderzoek en het trainen van AI. In lijn hiermee zette het Ministerie van VWS in op het grootschalig ongericht delen van gegevens, in strijd met het medisch beroepsgeheim en het recht op medische privacy. Op initiatief van Privacy First en onze maatschappelijke partners Platform Burgerrechten en stichting KDVP leidde dit in 2025 tot fundamentele maatschappelijke discussie over medische gegevensuitwisseling. Naast onze principiële zorgen over de EHDS werd deze discussie mede aangewakkerd door de introductie van Mitz, het nieuwe landelijke toestemmingsplatform voor het delen van medische gegevens. Uit meerdere onderzoeken bleek dat Mitz dezelfde fundamentele ontwerpfouten bevat als het eerder door de Eerste Kamer verworpen Landelijk Elektronisch Patiëntendossier (EPD). Zo kunnen zorgverleners zonder aanwezigheid van de patiënt diens toestemmingsinstellingen aanpassen, waardoor grootschalige en heimelijke inzage in medische dossiers mogelijk blijft. Privacy First [waarschuwde](#) dat hiermee het medisch beroepsgeheim structureel wordt ondermijnd en dat burgers feitelijk minder regie krijgen over hun gegevens.



Privacy First bracht deze governance-problematiek gedurende 2025 actief onder de aandacht van de Autoriteit Persoonsgegevens (AP). Ondanks uitgebreide documentatie, gesprekken en formele meldingen zag de AP vooralsnog echter geen aanleiding om in te grijpen. Ook bij het Ministerie van VWS oefende Privacy First druk uit op het staande beleid. We benadrukten daarbij dat *privacy by design* begint bij de ontwerpfase: zolang burgers en hun vertegenwoordigers geen zeggenschap hebben over de uitgangspunten van digitale zorgsystemen, blijven systeemrisico's bestaan die groter zijn dan bij het oude EPD.

Privacy First trad tevens krachtig naar buiten in de media. In uitzendingen van Pointer en NPO Radio 1 lichtten we toe waarom Mitz een bedreiging vormt voor medische vertrouwelijkheid. Privacy First presenteerde daarbij concrete alternatieven die wél aansluiten bij het medisch beroepsgeheim: systemen waarin artsen gericht en beperkt gegevens beschikbaar stellen, passend bij het actuele zorgtraject van de patiënt.

Daarnaast leidde de inbreng van Privacy First bij enkele ‘verzamelwetten’ over de verwerking van medische gegevens in 2025 tot diverse Kamervragen. Bij de NEN schreven we bovendien mee aan twee cruciale normen over gegevensuitwisseling in de zorg, ‘toestemming’ en ‘autorisatie’, waardoor een privacyvriendelijk alternatief voor grootschalige databeschikbaarheid behouden kan blijven. In dit verband benadrukte Privacy First o.a. dat iedere patiënt het recht heeft op bezwaar tegen de uitwisseling van zijn medische gegevens, inclusief alle toestemmingen daaromtrent. De enige manier om dit recht effectief te kunnen implementeren is door bezwaar en een bijbehorende (technische, absolute) blokkade bij de bron zelf, dus bij de arts. Dit is de enige manier om het medisch beroepsgeheim en het recht op medische privacy te kunnen garanderen.

Al met al kenmerkte het jaar 2025 zich voor Privacy First door intensieve beleidsbeïnvloeding, publieke voorlichting en maatschappelijke samenwerking. Privacy First bleef daarbij consistent pleiten voor transparante governance, veilige gegevensuitwisseling en een digitale zorginfrastructuur die de privacy van burgers respecteert.

4.3 Kinderen & privacy

In 2025 heeft Privacy First nadrukkelijk aandacht gevraagd voor de positie van kinderen en jongeren in de digitale samenleving. Aan de hand van verschillende artikelen op onze website hebben wij gewezen op de noodzaak om kinderrechten, privacy en autonomie als uitgangspunt te nemen bij de ontwikkeling en inzet van digitale technologieën. Daarbij zijn we ingegaan op de verleidingen van AI-chatbots, het sociale media gebruik onder jongeren en leerlingvolgsystemen in het onderwijs.

In een artikel over AI-chatbots benadrukten wij dat kinderen geen gewone gebruikers zijn en dat ontwikkelaars en aanbieders extra rekening moeten houden met hun kwetsbare positie. We benoemen de rol van ouders, school en overheid bij het gebruik van chatbots, maar roepen met name de aanbieders op om hun verantwoordelijkheid te nemen. Daarnaast hebben wij aandacht gevraagd voor de impact van sociale media op jongeren. We hebben niet alleen de risico's benoemd van het gebruik door jongeren maar ook de kansen op het gebied van sociale verbondenheid, identiteitsontwikkeling en expressie. Privacy First sprak

zich uit tegen een generiek verbod op sociale media voor kinderen onder de 16 jaar en benadrukte juist de verantwoordelijkheid van de platforms om een veilige digitale omgeving te bieden aan jongeren. In een artikel over leerlingvolgsystemen zoals Magister en Somtoday gingen we in op de praktijk bij scholen om gegevens over leerlingen zoals over absentie of resultaten (direct) te delen met de ouders. We benadrukten de autonomie en privacy van leerlingen in het voortgezet onderwijs en riepen scholen op om zorgvuldiger om te gaan met leerling-gegevens.

Tevens bleek in 2025 uit technisch onderzoek door Privacy First (in samenwerking met de Hogeschool Utrecht) in digitale babyfoons vooral het belang van digitale soevereiniteit. Afhankelijkheid van niet-Europese partijen en buitenlandse wetgeving zorgt er immers voor dat we geen idee hebben of de privacy van onze kinderen gegarandeerd is.

De grote lijn is helder: technologische mogelijkheden mogen niet ten koste gaan van de rechten en ontwikkeling van kinderen. Privacy First blijft zich inzetten voor een digitale omgeving waarin kinderrechten centraal staan en structureel worden meegenomen in beleid, ontwerpkeuzes en toepassingen.



4.4 Overige onderwerpen

Gedurende 2025 was er o.a. kritische lobby van Privacy First inzake het wetsvoorstel transparantie en tegengaan ondermijning door maatschappelijke organisaties (Wtmo). Door dit wetsvoorstel dreigde immers vooral het goede functioneren van het maatschappelijk middenveld (stichtingen, verenigingen, goede doelen) te worden ondermijnd. Mede door de kritische inbreng van Privacy First (o.a. tijdens een parlementaire deskundigenbijeenkomst in november 2025) werd dit wetsvoorstel door de Eerste Kamer verworpen.

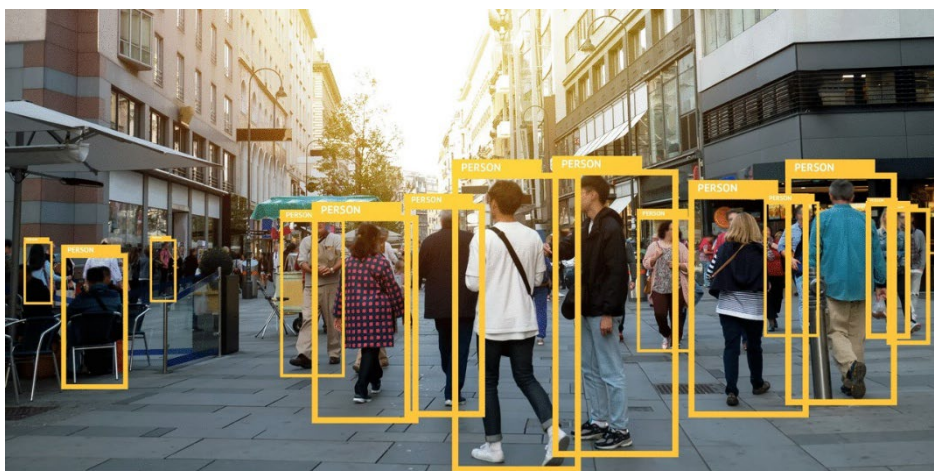
Shrinking space
for civil society



Deskundigenbijeenkomst Eerste Kamer met o.a. Privacy First inzake de Wet transparantie en tegengaan ondermijning door maatschappelijke organisaties (Wtmo, 25 november 2025, Den Haag).

Privacy First zorgde in 2025 tevens voor aanhoudende druk richting de Eerste Kamer ter invoering van de mogelijkheid van bezwaar en beroep bij de zogeheten “persoonsgerichte aanpak” (PGA), dit in lijn met een door Privacy First gesteunde eerdere, baanbrekende rechtszaak daaromtrent bij de Raad van State. Anno 2026 staat dit onderwerp bij de Eerste Kamer (en NCTV) immer actief op de agenda.

Daarnaast was Privacy First in 2025 mede-ondertekenaar van brieven van de organisatie European Digital Rights (EDRi) i.v.m. actuele zorgen rond encryptie en mogelijke herziening van de AVG (EU “Digitale Omnibus”). Over dit laatste onderwerp participeerde Privacy First ook kritisch in een consultatie van de Europese Commissie. Tevens riepen we in het kader van de Nederlandse nationale verkiezingen politieke partijen op om digitale soevereiniteit en privacy in hun verkiezingsprogramma’s op te nemen.



5. Rechtszaken

Als maatschappelijke organisatie gaat het Privacy First erom zo effectief mogelijk te opereren met de beperkte middelen die wij hebben. Als stille diplomatie en politieke lobby onvoldoende effectief blijken, voert Privacy First daarom principiële rechtszaken tegen wetgeving en beleid die tot grootschalige privacyschendingen leiden. De afgelopen jaren deed Privacy First dit met succes tegen de centrale opslag van ieders vingerafdrukken onder de Paspoortwet, de opslag van ieders telecommunicatie-data onder de Wet bewaarplicht telecommunicatiegegevens en massale risicoprofilering van burgers door het Systeem Risico Indicatie (SyRI). Privacy First voert dergelijke zaken bij voorkeur in coalitieverband en met pro bono ondersteuning (of externe sponsoring) door geschikte advocatenkantoren.



© Guus Schoonewille

5.1 Rechtszaak tegen ANPR massa-surveillance

Begin 2019 trad in Nederland een nieuwe wet inzake Automatische Nummerplaat Herkenning (ANPR) in werking. Onder deze wet (art. 126 jj Sv.) worden sindsdien door ANPR-camera's boven de snelwegen de kentekens en locaties van miljoenen auto's (oftewel ieders reisbewegingen) continu 4 weken in een centrale politiedatabank opgeslagen voor o.a. opsporing en vervolging. Dit is totaal niet noodzakelijk, volstrekt disproportioneel en bovendien ineffectief, zo bleek de afgelopen jaren uit diverse onderzoeken. Toezicht ontbreekt en het systeem kan eenvoudig worden misbruikt. De huidige ANPR-wet vormt daarom een massale privacyschending en hoort niet thuis in een vrije democratische

rechtsstaat. Privacy First voert sinds 2021 een [rechtszaak](#) tegen de Staat om de ANPR-wetgeving onrechtmatig te laten verklaren wegens strijd met Europees privacyrecht. Via Pro Bono Connect heeft Privacy First het advocatenkantoor CMS ingeschakeld om deze rechtszaak (kort geding en bodemprocedure) voor ons te voeren. Deze zaak wordt tevens gesteund door het Digital Freedom Fund.

Mede onder druk van deze rechtszaak heeft de Nationale Politie "*privacy by design*" geïmplementeerd in de zin dat voorruitens van auto's voortaan automatisch worden geblindeerd in ANPR-camerabeelden, waardoor inzittenden niet meer zichtbaar zijn. Onze ANPR-zaak heeft de afgelopen jaren ook de nodige media-aandacht gekregen, waardoor het kritische bewustzijn over massasurveillance is toegenomen.

Begin 2024 verklaarde de rechtbank Den Haag Privacy First ontvankelijk in de bodemprocedure. Dit tussenvonnissen heeft sindsdien belangrijke precedentwerking voor vergelijkbare zaken, zeker nu vanuit de Nederlandse politiek de mogelijkheden voor belangenorganisaties om rechtszaken te voeren steeds meer beperkt dreigen te worden. Inhoudelijk stelde de rechtbank Privacy First vervolgens echter in het ongelijk. Privacy First heeft daarna hoger beroep ingesteld bij het Hof Den Haag en tevens een reeks Woo-verzoeken ingediend bij diverse overheidsorganisaties.



De rechtszitting in hoger beroep bij het Hof heeft in juli 2026 plaatsgevonden. Privacy First hoopt en verwacht met deze zaak een kritisch Europees precedent te kunnen creëren.

5.2 Coalitiezaak tegen Amerikaanse overname van DigiD-leverancier

In november 2025 werd bekend dat de Nederlandse DigiD-leverancier Solvinity zou worden overgenomen door het Amerikaanse tech-bedrijf Kyndryl. Onder Amerikaanse wetgeving zou de Nederlandse vitale infrastructuur achter DigiD (en daarmee gevoelige persoonsgegevens van de gehele Nederlandse bevolking) daardoor binnen het bereik van de Amerikaanse overheid komen. In januari 2026 diende de nieuwe stichting Firewall daarom samen met een groep wetenschappers, journalisten, opiniemakers en Privacy First een verzoek in bij het Bureau Toetsing Investerings (BTI) en de verantwoordelijke minister van Economische Zaken om de overname van Solvinity door Kyndryl te stoppen en als belanghebbende partijen te worden erkend, gevolgd door een [rechtszaak](#) hierover bij de rechtbank Rotterdam.

Onze coalitie wist zich daarbij gesteund door het feit dat de politieke en maatschappelijke weerstand tegen een Amerikaanse overname van Solvinity inmiddels massale vormen had aangenomen in alle geledingen van de Nederlandse samenleving. In mei 2026 was de rechtszitting bij de rechtbank Rotterdam. Een week later vond een positieve doorbraak plaats: de overname van Solvinity door Kyndryl werd door de staatssecretaris van Economische Zaken verboden. Dit ter bescherming van het publieke belang (privacy en staatsveiligheid). Naar aanleiding van het overnameverbod hebben stichting Firewall en Privacy First c.s. vervolgens besloten om de lopende rechtszaak bij de rechtbank Rotterdam in te trekken; dit wegens het ontstane gebrek aan actueel procesbelang.

Het overnameverbod is volgens Privacy First het enige juiste besluit dat de Nederlandse regering had kunnen nemen. Elke andere uitkomst was in onze optiek onverantwoord en onrechtmatig geweest. Privacy First hoopt dat dit besluit een precedent schept om ook kritisch te kijken naar het gebruik van andere diensten van buiten Europa. Dit kan een positieve kentering in de geschiedenis vormen.

Naast stichting Firewall en Privacy First bestond de coalitie uit initiatiefnemer Eric Smit, Esther van Egerschot, Maxim Februari, Feliene Hermans, Bert Hubert, Joris Luyendijk, Caroline Nevejan, Reijer Passchier, Jelle Postma, Sander Schimmelpenninck, Karin Spaink, Marleen Stikker en Kees Verhoeven. Deze zaak werd low bono gevoerd door Corten De Geer Advocaten en Boekx Advocaten.

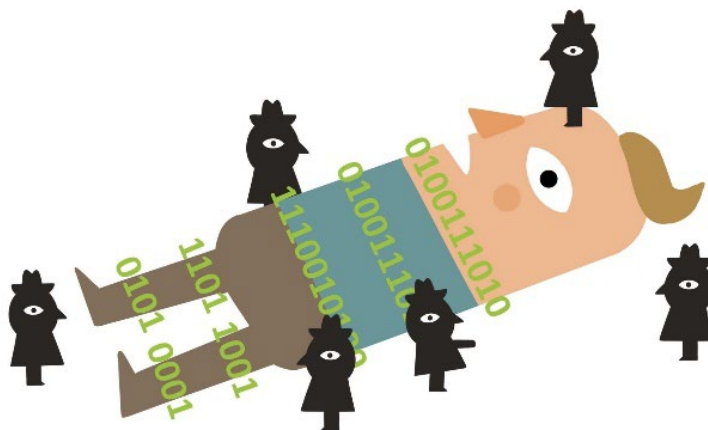
Stichting Firewall en Privacy First zijn de verdere ontwikkelingen sindsdien kritisch blijven volgen en hebben recent (op uitnodiging van de rechtbank Rotterdam) geïntervenieerd in een zaak van Solvinity tegen het overnameverbod. Een vonnis in deze zaak wordt spoedig verwacht.



5.3 Overige rechtszaken

Privacy First steunt incidenteel tevens rechtszaken van andere organisaties en individuele burgers, mits dergelijke zaken van dusdanige aard zijn dat onze steun daarbij onontbeerlijk is, dit in het belang van de juridische ontvankelijkheid en positieve precedentvorming, maatschappelijke bewustwording of beïnvloeding van relevante wetgeving en beleid. Voorbeelden hiervan zijn de rechtszaken van de Arnhemse privacy-activist Michiel Jonker ten behoeve van anoniem reizen met het openbaar vervoer en het recht op contante betaling in de bioscoop c.q. openbare gelegenheden, de massaclaim van The Privacy Collective tegen Oracle & Salesforce (illegale datahandel), de zaak van Gilles Ampt over kentekenparkeren en de anonieme blauwe parkeerschijf (gemeente Wageningen) en de rechtszaak van een coalitie van o.a. het Platform Burgerrechten, psychiaters, psychologen en cliënten in de GGZ tegen de Nederlandse Zorgautoriteit (medische privacy en beroepsgeheim). In deze zaken geeft Privacy First bijvoorbeeld advies en kunnen wij zogeheten *amicus curiae* steunbrieven indienen. Dergelijke rechtszaken leiden vaak ook tot mediapublicaties en kritische vragen op gemeentelijk of nationaal politiek niveau.

De coalitie van maatschappelijke organisaties (waaronder Privacy First) die eerder de baanbrekende rechtszaak tegen het Systeem Risico Indicatie (SyRI) won riep de afgelopen jaren de Eerste en Tweede Kamer tevergeefs op om de **Wet Gegevensverwerking Samenwerkingsverbanden (WGS)** te verwerpen. In de optiek van deze coalitie vormt massale risico-profilering onder de WGS immers SyRI in het kwadraat ("Super SyRI") en een blauwdruk voor nieuwe toeslagenaffaires. Inmiddels hebben het Platform Burgerrechten en Privacy First een gezamenlijke rechtszaak ter fundamentele toetsing van de WGS aan Europees privacyrecht in voorbereiding.



6. Claimstichting CUIC

CUIC is een onafhankelijke non-profit organisatie en staat voor Consumers United in Court, ook uit te spreken als 'CU in Court' (*see you in court*). CUIC heeft als missie de privacy van consumenten te beschermen en kan daartoe procederen onder de nieuwe Wet afwikkeling massaschade in collectieve actie (Wamca), waarbij de krachten van consumenten gebundeld worden. CUIC is mede opgericht door Privacy First en de Europese privacy-organisatie None of your business (Noyb).

De eerste zaak van CUIC wordt sinds 2024 gevoerd tegen het techbedrijf Avast dat jarenlang het online surfgedrag van miljoenen mensen onrechtmatig verzamelde en doorverkocht. Deze zaak loopt bij de rechtbank Amsterdam. De tweede zaak van CUIC is een collectieve procedure tegen Odido vanwege het recente datalek waarbij data van meer dan 6 miljoen Nederlanders werden buitgemaakt. Deze zaak draait niet alleen om die hack zelf, maar ook om de laksheid waarmee Odido is omgesprongen met gevoelige gegevens van haar klanten en oud-klanten. Zie voor meer informatie over CUIC en beide zaken <https://cuic.eu>.



7. Communicatie

7.1 Massamedia

Gemiddeld verscheen Privacy First in 2025 enkele keren per week in de media. Voorbeelden hiervan waren interviews bij RTL Z (over Meta en AI), SBS6 (drones, slimme deurbellen), Radio 1 (o.a. Persoonsgerichte Aanpak (PGA), DNA bij *cold cases*, nieuw landelijk Elektronisch Patiëntendossier, cybersecurity), BNR Nieuwsradio (Chinese AI-chatbot DeepSeek, digitale soevereiniteit, digitale euro), ANP, NRC, Volkskrant, Trouw en Algemeen Dagblad (o.a. bancaire sleepnet, EU “chat control”, digitale euro, diverse datalekken), NU.nl (Europees Entry/Exit grenscontrolesysteem, datalek bij Bevolkingsonderzoek), regionale dagbladen (anonieme blauwe parkeerschijf), RTL Nieuws (surveillance bij demonstraties, publieke schandpalen), iBestuur en Security.nl (o.a. Europese digitale identiteit, slimme deurbellen), Belgisch dagblad De Morgen (slimme deurbellen), Amerikaanse nieuwssite TechCrunch (Signal), Wereld van Filantropie (Wtmo) en Statewatch (Europese anti-witwaswetgeving). Naast verzoeken om interviews wordt Privacy First regelmatig door journalisten benaderd om achtergrondinformatie en onderzoekstips, soms ook door buitenlandse media. Vermeldenswaardig is tevens de publicatie (eind 2025) van een bijzonder boek van Bob Hardus waarin o.a. Privacy First het podium kreeg: *De Prijs voor Privacy – Van de Stasi tot Big Tech: hoe surveillance ons leven bepaalt*.



Televisie-interview met Privacy First over drones (Shownieuws, 19 juni 2025) © SBS6

7.2 Internet

De tweetalige website (NL/ENG) van Privacy First <https://www.privacyfirst.nl> vormt ons primaire nieuws- en opiniekanaal. Op social media is Privacy First voornamelijk actief op [LinkedIn](#) en sinds kort tevens op [BlueSky](#) en [Mastodon](#). (Op X is Privacy First sinds begin 2026 niet meer actief.) Daarnaast verschijnen vrijwel al onze persberichten en artikelen bij het online vakblad PONT Data & Privacy en vindt u ons ook bij het privacyvriendelijke platform [Quodari](#). Wilt u graag op de hoogte blijven van alle ontwikkelingen rondom Privacy First? Meldt u dan aan voor onze maandelijkse nieuwsbrief en periodieke uitnodigingen via <https://privacyfirst.nl/nieuwsbrieven/> !

8. Organisatie

Privacy First is een onafhankelijke, ANBI-erkende stichting die van oudsher grotendeels uit professionele vrijwilligers bestaat, soms met tijdelijk personeel en incidentele inhuur. Doel van Privacy First in de periode 2026–2028 is onze ontwikkeling richting een compacte, flexibele organisatie met meer vaste medewerkers.

Het bestuur van Privacy First bestond in 2025 uit de volgende personen:

- Sander Klous (voorzitter)
- Haykush Hakobyan (secretaris)
- Marvin Biljoen (penningmeester)
- Wilmar Hendriks (algemeen bestuurslid; tevens bestuursvoorzitter CUIIC; beide tot november 2025)
- Steven Derks (algemeen bestuurslid)
- Floris Lazrak (algemeen bestuurslid).

Onze bestuursvergaderingen vonden in 2025 gemiddeld maandelijks plaats.

De Raad van Advies (RvA) van Privacy First bestond in 2025 uit de volgende personen, op persoonlijke titel:

- Paul Sloomaker (vice-president Monitoring & Reporting, KPN)
- Eliëtte Vaal (ICT & privacy advocaat, The Data Lawyers)
- Bart Schellekens (ICT & Privacy jurist, Ministerie van Financiën)
- Dennis Groot (CEO, Abykys)
- Paul Dam (Adviseur Recht & Digitale technologie, Lex Digitalis).

Inmiddels is onze RvA deels vernieuwd. Onze RvA komt enkele malen per jaar bijeen met ons bestuur en geeft tevens ongevraagd advies.

De groep vrijwilligers van Privacy First bestaat voornamelijk uit professionals die Privacy First structureel ondersteunen, zowel inhoudelijk (verschillende privacy-thema's) als organisatorisch (ICT, PR, fotografie etc.) en juridisch (onderzoek en advies). Daarnaast beschikt Privacy First over een uitgebreid netwerk van experts uit alle hoeken van de samenleving, variërend van wetenschappers, juristen en ICT'ers tot journalisten, politici en ambtenaren.

9. Financiën

Stichting Privacy First is voor haar werkzaamheden grotendeels afhankelijk van individuele donaties en steun van fondsen, bedrijfsdonateurs en advocatenkantoren. De afgelopen jaren heeft Privacy First meerdere fondsen aan zich kunnen verbinden ter ontwikkeling van nieuwe projecten en ter versterking en verduurzaming van onze organisatie en activiteiten. Privacy First heeft daarbij een voorkeur voor algemene of institutionele steun ("core funding") i.p.v. projectsteun. Fondsen die ons de afgelopen jaren steunden waren o.a. Stichting Democratie & Media, Adessium, SIDN Fonds, Digital Freedom Fund, Sub3 en Stichting Goeie Grutten. Naast financiële steun door individuele donateurs en fondsen staat Privacy First ook open voor sponsoring door bedrijven, mits Privacy First volledig vrij en onafhankelijk kan blijven functioneren. Zo wordt Privacy First bijvoorbeeld al jaren gesteund door Voys Telecom. Onze jaarlijkse Nationale Privacy Conferentie wordt gesponsord door ECP en onze Nederlandse Privacy Awards worden gesponsord door NordVPN. Zou uw organisatie graag ook Privacy First willen sponsoren? Neem dan contact met ons op!

Vast beleid van Privacy First is om alle inkomsten zoveel mogelijk te besteden aan inhoudelijk relevante zaken en de operationele kosten zo laag mogelijk te houden. Onze communicatie verloopt daartoe (ook telefonisch) grotendeels via internet. Ondersteunende werkzaamheden worden grotendeels uitgevoerd door professionele vrijwilligers. Ons kantoor aan de Nieuwe Herengracht in Amsterdam deelden wij tot begin 2026 met claimstichting CUIC; sindsdien is Privacy First gevestigd in het Keynesgebouw in Amsterdam Nieuw-West. Evenementen van Privacy First worden bij voorkeur georganiseerd op externe gesponsorde locaties. De processtukken in onze rechtszaken worden door Privacy First ondersteund door eigen feitelijk en juridisch onderzoek. Vast beleid van Privacy First is bovendien om onze rechtszaken bij voorkeur pro bono en in coalitieverband te voeren via Pro Bono Connect, via het Public Interest Litigation Project (PILP NJCM) of met externe financiering. Dit om onze

kosten en financiële risico's zo laag mogelijk te houden en de kans op juridische winst te verhogen. Op deze manier komt iedere gedoneerde euro zo effectief mogelijk ten goede aan de privacy van iedere Nederlander.

Hieronder treft u ons financiële jaaroverzicht 2025 aan. Voor een volledig overzicht verwijzen wij u naar onze jaarrekening op onze website.

Jaaroverzicht	2025		2024	
Inkomsten:				
Donaties en fondsen	€	123.378	€	182.978
Uitgaven:				
HR-kosten	€	86.057	€	142.575
Juridische kosten	€	-	€	-
Huisvesting	€	9.804	€	9.076
Publieksactiviteiten	€	3.101	€	8.947
Verzekeringskosten	€	1.861	€	1.455
Websites, marketing en ICT	€	15.463	€	22.473
Kantoorkosten	€	4.874	€	4.275
Representatiekosten	€	1.382	€	764
Administratiekosten	€	11.589	€	2.408
Overige algemene kosten	€	1.057	€	5.693

10. Vooruitblik 2026 en verder

Voor de komende jaren streeft Privacy First naar een samenleving waarin:

- politici, burgers, ondernemers en ambtenaren zich bewust zijn van de waarde van onze grondrechten en persoonlijke autonomie;
- mensen zelf het gezag hebben over hun eigen levens, de gegevens die daaruit voortkomen (data soevereiniteit) en zich anoniem kunnen bewegen;
- dit in wetgeving, maar vooral ook in het ontwerp van technologie verankerd is (*privacy by design*);
- en we gegevens op verantwoorde wijze kunnen delen voor persoonlijke, maatschappelijke en economische doeleinden.

Sterk internationaal netwerk

Wetgeving uit Brussel heeft een enorme impact op onze maatschappij. Per thema bouwen we coalities op, of sluiten we aan bij bestaande. Hiermee krijgen we meer slagkracht. We verdelen de werklast, worden sneller, slimmer en effectiever.

Privacy kennisleider

Afgelopen jaren hebben we bekendheid opgebouwd. Media weten ons te vinden. We hebben een netwerk bij de overheid en in de politiek. Dit breiden we verder uit. Dat doen we strategisch, doordacht en opportunistisch. Nederlandse onderwerpen koppelen we zoveel mogelijk aan zaken in de Brusselse pijpleiding.

Verjonging en verbreding

Jongeren vinden privacy belangrijk, maar komen nog te weinig voor in onze achterban en er zijn nog steeds mensen die denken dat ze “niets te verbergen hebben”. We verjongen en verbreden onze achterban, buiten onze comfortzone, met gerichte projecten in meerdere segmenten.

Voor meer informatie over onze huidige plannen en mogelijke projecten tot 2030 zijn fondsen en bedrijfsdonateurs van harte welkom om [contact](#) met Privacy First op te nemen!

Wilt u Privacy First graag steunen? Maak dan een donatie over naar IBAN: NL95ABNA0495527521 (BIC: ABNANL2A) t.n.v. Stichting Privacy First te Amsterdam, of steun ons via de [donatiepagina](#) op onze website. Privacy First is erkend als Algemeen Nut Beogende Instelling (ANBI). Uw giften aan Privacy First zijn daarom belastingaftrekbaar.





Postbus 16799

1001 RG Amsterdam

Telefoon: 020-8100279

Email: info@privacyfirst.nl

Website: www.privacyfirst.nl

Privacy First is ingeschreven in het Stichtingenregister van de KvK Amsterdam onder nr. 34298157.
RSIN/fiscaal nummer: 819211710.