Burgerrechtenvereniging VRIJBIT

www.vrijbit.nl





Maar om dat zo te houden gaat niet vanzelf.

Jaarverslag 2018 Burgerrechtenvereniging Vrijbit 10 mei 2019

Inhoudsopgave

Inhoudsopgave	pagina 1
Inleiding	pagina 2
Algemene ontwikkelingen in 2018	pagina 3
Actuele en doorlopende kwesties	pagina 10
Activiteiten van Vrijbit in 2018	pagina 16
Intern functioneren 2018	pagina 24
Financieel jaaroverzicht 2018	pagina 29

Inleiding

In dit jaarverslag geeft Burgerrechtenvereniging Vrijbit een schets van de ontwikkelingen op het gebied van de privacybescherming, een overzicht van verrichte werkzaamheden, een blik op het intern functioneren van de vereniging en de financiële verantwoording over het jaar 2018.

Door middel van dit jaarverslag legt het bestuur verantwoording af tegenover de leden en donateurs.

Tevens verschaft het verslag informatie over de stand van zaken aangaande de strijd, om het behoud van het recht op persoonlijke vrijheid in 2018, en de rol die Vrijbit daarin speelde.

Het jaarverslag zal, na goedkeuring tijdens de Algemene Ledenvergadering, op de website www.vrijbit.nl worden gepubliceerd. Op aanvraag is een papieren versie verkrijgbaar.

Algemene ontwikkelingen in 2018

- 2018 ging, net als voorgaande jaren, de geschiedenis in als een jaar waarin we geconfronteerd werden met een gigantische hoeveelheid nieuwe berichten en ontwikkelingen in het kader van de Privacy.
- Zoals, bijna dagelijks, nieuwe informatie over datalekken en misbruik van persoonsgegevens.
- Over nieuwe technologische ontwikkelingen.
- Nieuwe, en recent ontdekte, gevaren van online communicatie die een bedreiging vormen voor de bescherming van personen en het functioneren van instanties, bedrijven en zelfs vitale sectoren van de samenleving.
- Cijfers met betrekking tot het aantal mensen dat als niet digivaardig wordt aangeduid en door de steeds intensiever gedigitaliseerde maatschappij buitengesloten dreigen te raken.
- Informatie over falende overheidsinstanties en bijbehorende mislukte ICT-systemen.
- Een nauwelijks bij te benen berichtenstroom over de voortgang van (nieuwe, aangepaste, voorgenomen of afgeschoten) wet-en regelgeving.
- Informatie in zake juridische procedures tegen privacyaantastingen en inbreuken op het recht op een privéleven.

Daarnaast ook aandacht voor initiatieven, publicaties en wetgeving die beoogden de macht van de grote internetgiganten in te perken, een beter kader te scheppen voor de bescherming van persoonsgegevens en pogingen om mensen niet alleen bewust te maken van welke data er allemaal over hen verzameld wordt en wat daarmee gebeurt, maar hen zich daar ook terughoudender door te laten gedragen.

We lichten er hierna een paar in het oog springende zaken uit:



Social media De online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen trokken volop aandacht. Met berichtgeving over de internetverslaving en de gevolgen daarvan qua gezondheidsklachten, de toename van online pesten, risico op screening door werkgevers en overheden, criminele afpersing,gevolgen van nepnieuws en de gevaren van ‘appen’ en bellen door verkeersdeelnemers.

‘In Nederland is WhatsApp nog altijd het grootste social media platform. Met 11.5 miljoen gebruikers worden ze op de voet gevolgd door Facebook met 10.8 miljoen gebruikers. De grootste stijger dit jaar is Instagram. 4.1 miljoen Nederlanders maken gebruik van Instagram, waarvan 2.1 miljoen dagelijks. Dat is 40% meer dan in 2017. Instagram heeft nu bijna net zoveel dagelijkse gebruikers als YouTube (2.1 miljoen)’.

Bron: Nationale Social Media Onderzoek 2018- Newcom januari 2018
https://www.newcom.nl/index.php?page=socialmedia2018

Facebook trok veel aandacht. Met nagenoeg wekelijks nieuwe schandalen over de manier waarop het bedrijf wereldwijd de gegevens van hun miljarden gebruikers verzamelde en vermarktte. Wat begin van het jaar begon met de affaire rond de verkoop van de persoonsgegevens van 87 miljoen gebruikers aan het Britse bedrijf Cambridge Analytica die daarmee probeerde de Amerikaanse verkiezingen te beïnvloeden en eindigde met het lek van de privéfoto's van zo'n 6,8 miljoen gebruikers die mogelijk in handen zijn gekomen van applicatie- ontwikkelaars op het platform. En berichtgeving over de manier waarop het Amerikaanse Congres en de Europese Unie (tamelijk vruchteloos) probeerden om de invloed van deze datagrootmacht, met 2,32 miljard actieve gebruikers een omzet van 55 miljard dollar per kwartaal, in te perken.

Google, het bedrijf wat naast de zoekmachine ook eigenaar is van videoplatform YouTube, het besturingssysteem Android maakte, diensten zoals Google Maps en Gmail beheert, en zich bezig houdt met drones, slimme apparaten voor in huis, zelfrijdende auto's, gezondheidszorg en kunstmatige intelligentie, lag eveneens onder vuur. Dit vanwege Googles datahonger en het misbruik maken van haar marktpositie. *In 2017 had de Europese Commissie het bedrijf al een boete van 2,4 miljard euro opgelegd voor oneerlijke prijsvergelijking in de zoekmachine. In juli 2018 volgde een tweede boete, ditmaal van 4,3 miljard euro omdat Google afnemers van Android dwong om de Google-app en de app van zijn internetbrowser Chrome op smartphones te installeren.*



Datahonger van de overheid en semi-overheden was eveneens een in allerlei vormen terugkerend hoofdpijn dossier. Met name de gigantische controledrang in de zorgsector en het onderwijs kwamen telkens aan de orde. Vanwege de privacyaantastingen en wegens de regeldruk die contraproductief werkte waar het in de bedoeling lag om betere prestaties of fraudebestrijding te bewerkstelligen.

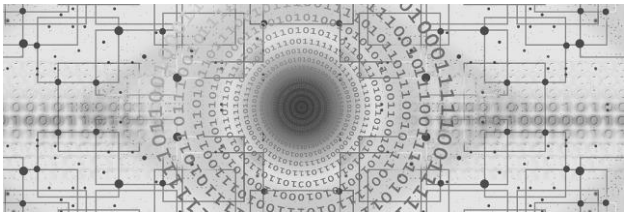
En, mede dankzij de rechtszaak tegen het Systeem Risico indicatie (SYRi), de voorlichting over de nieuwe Wet op de inlichtingen-en veiligheidsdienst (Wiv-2017) en de concrete voorbeelden van hoe het sociaal kredietstelsel in China functioneert, werd in steeds bredere kring bekend hoe de koppeling van data:

- Het steeds makkelijker maakte om bepaalde gegevens, ook als ze zijn gespeudonimiseerd of niet rechtstreeks gekoppeld mogen worden, tot een persoon te herleiden. *Waardoor op zichzelf onschuldige tamelijk anonieme gegevens via indirecte identificatiemethoden alsnog zoveel informatie over iemands gedrag kunnen geven dat ze als persoonsgegevens moeten worden aangemerkt.*
- In toenemende mate werden ingezet voor profiling en risico analyse. *Waarbij het voor veel mensen die zich daar voordien weinig bij konden voorstellen een stuk concreter werd wat daar, behalve de al wel bekende getagete/gerichte reclame, de gevolgen van kunnen zijn.*
- Zich steeds verder onttrekt aan wet-en regelgeving die geen gelijke tred hielden bij technologische mogelijkheden.
- De wijze van verwerken door automatische softwaresystemen en geheime algoritmen het steeds moeilijker maakte voor betrokkenen om zicht te kunnen houden op wat er met hun gegevens gebeurd. Hetgeen bij de inzet van zelflerende systemen door kunstmatige intelligentie(AI) ook voor de bewerkers van de data zelf gold.



Digitalisering vormde de rode draad in nagenoeg alle privacy kwesties. Een eindeloze reeks datalekken en hacking van digitale bestanden vormde daar slechts één aspect van. Een aspect overigens dat op zich al belangrijk genoeg was om duidelijk te maken hoe kwetsbaar de afhankelijkheid van digitalisering zowel de individuele mens als vitale onderdelen van de samenleving maakte.

> In 2018 werden er 20.881 datalekken gemeld aan de Autoriteit Persoonsgegevens (AP). De meeste datalekken werden gemeld vanuit de sectoren gezondheid en welzijn (29%), financiële dienstverlening (26%) en openbaar bestuur (17%). Deze percentages zijn vergelijkbaar met de percentages van de voorgaande jaren. Net als in 2017 was in 2018 het meest voorkomende type datalek het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger (63% van de meldingen). Dit kan bijvoorbeeld een brief met gevoelige gegevens zijn die bij de verkeerde persoon terecht is gekomen en is geopend. Het kwijtraken of de diefstal van een gegevensdrager zoals een laptop of usb-stick (14%) is daarna het meest voorkomende type datalek. De soorten gegevens die het meest vrijkwamen bij een datalek waren NAW-gegevens, BSN en medische gegevens. Bron jaarverslag AP 2018

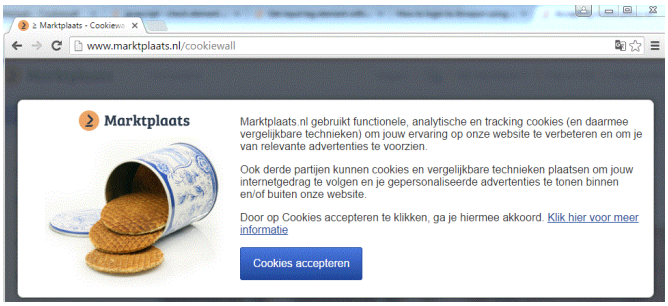


Die kwetsbaarheid gold eveneens voor het steeds verder verknoopt raken van alle sectoren van de samenleving. Waardoor het datapakket aan gegevens over bepaalde personen en groepen zich exponentieel verder uitbreidde. Met als gevolg dat mensen in toenemende mate als equivalent van hun datapakket kunnen worden beschouwd en behandeld. Met alle gevolgen van dien voor het verder kunnen standaardiseren en automatiseren van beleidsbeslissingen en bijvoorbeeld de dienstverlening.

Het vormde daarbij dit jaar een schrale troost dat er eindelijk erkenning leek te komen voor het standpunt dat Vrijbit al 10 jaar uitdraagt. Namelijk dat het versleutelen van persoonsgegevens door pseudonimisering niet kán voldoen om iemands anonimiteit te garanderen. En dat het uiterst kwalijk is als dataverwerkers blijven doen voorkomen dat pseudonimiseren van data gelijk zou staan aan anonimiseren waardoor gegevens niet meer tot een bepaalde unieke persoon te herleiden zouden zijn. Dit werd dan weliswaar in 2018 alom erkend binnen de overheid, het bedrijfsleven en de rechtspraak, maar leidde doorgaans vervolgens niet tot de inzet op anonimisering bij de bron, het minder vastleggen van gegevens (dataminimalisatie) of in de opbouw fase van dataverwerkingsystemen compartimeren van datastromen. In tegendeel zelfs. Waar dit nieuwe bewustzijn doorbrak dat veel data, die voorheen niet als persoonsgegevens werden beschouwd, wel degelijk als zodanig moesten worden aangemerkt en bij wet als zodanig dienden te worden beschermd, leidde dat in veel gevallen juist tot een heel andere reactie. Er

werd namelijk vervolgens volop ingezet op strategieën die ten doel hadden om de praktijk van het onrechtmatig verzamelen en koppelen van data, alsnog te 'rechtvaardigen'. Zoals door het wijzigen van de wettelijke grondslag waarop data verwerkt mogen worden, het uitbreiden van bevoegdheden van dataverwerkers, het beschermen van verwerkingsmethoden als bedrijfsgeheim enz. Ook de presentatie van schijnoplossingen als zou door de inzet van Privacy Impact Assesments (PIA's) of slechts vermelden van een deel van iemands postcode een betere privacybescherming bieden deden volop opgang.

Bedrijven, van zorgverzekeraars tot internetgiganten, zetten daarbij in op de bescherming van hun bedrijfsprocessen en ze hanteerden ondoorgrondelijke privacyvoorwaarden. *Waardoor het voor de mensen om wie het gaat onmogelijk werd gemaakt om zicht te kunnen krijgen op wat er over hen werd vastgelegd, hoe dat gebeurde, wie daarover kon beschikken, wie verantwoordelijk is en waar de data voor gebruikt werden (en konden gaan worden).*



Ook probeerde men vast te houden aan de constructie dat bijvoorbeeld het verlenen van toestemming voor tracking cookies werd afgedwongen door websites enkel toegankelijk te maken als mensen zich akkoord verklaarden, ondanks het feit dat cookiewalls bij invoering van de AVGwet expliciet verboden zijn.

Let op: het verbod op cookiewalls ziet niet alleen op het plaatsen van cookie, maar ook daarmee vergelijkbare technieken waarvoor eveneens toestemming gevraagd moet worden. Bron: https://www.autoriteitpersoonsgegevens.nl

Zo ook werden toestemmingsvereisten voor klantonderzoeken van klanten afgetroggeld door het bevoordelen van klanten die hun kortingskaart personaliseren.



Deze voordelen laat je toch niet schieten? Wist je dat je veel meer uit je Bonuskaart kunt halen? Door je Bonuskaart persoonlijk te maken ontvang je wekelijks vele extra's waarvan wij denken dat ze voor jou relevant zijn. En hoe vaker je je Bonuskaart laat scannen, hoe beter we je leren kennen. Zo kunnen we voordeel bieden dat bij je past. Een Ah.nl-profiel is nodig om je Bonuskaart te activeren. Ga naar de speciale Bonuskaart activatiepagina en vul je gegevens in. Bron:https://www.ah.nl/bonuskaart

Overheden en particuliere bedrijven die zogenaamde publieke taken uitvoeren zetten daarbij tevens in op aanpassen van de wettelijke grondslagen om illegale praktijken alsnog 'gelegaliseerd' te kunnen voortzetten. Zoals middels het gegoochel van termen als toestemmingsvereiste. En het wijzigen van wet- en regelgeving door op het verzamelen en verwerken van data het etiket te plakken dat dit noodzakelijk zou zijn vanwege begrippen als 'staatsveiligheid', 'openbare orde' of 'fraudebestrijding in het kader van het betaalbaar houden van de Zorg'.

Doelstellingen die per definitie te ruim geformuleerd werden en niet met feiten onderbouwd om te kunnen voldoen aan de eisen die het Europees Verdrag voor de Rechten van de Mens stelt aan het onder voorwaarden van overheidswege inbreuk mogen maken op de fundamentele rechten. Zoals het recht op privacy en lichamelijke integriteit. Recht op gewetensbezwaar/levensovertuiging. Recht op een eerlijk proces gebaseerd op het onschuldprincipe. En het recht op informatie en vrije communicatie.

Rechten zoals vastgelegd in de Grondwet , het Europese Verdrag voor de Rechten van de Mens en Handvest van de Grondrechten van de Europese Unie, die formeel prevaleren boven nationale wetgeving. Maar waar steeds weer door de regering succesvol inbreuk op werd gemaakt omdat de politici uit de Tweede- en Eerste Kamer zulke wetsvoorstellen geen halt toe riepen en toestonden dat holle kaderwetgeving, buiten het democratisch debat om, zou worden ingevuld via ministeriële regelingen en algemene maatregelen van bestuur.

Burgerrechten die door de eigen overheid, stelselmatig en op grote schaal, werden overtreden als exponent van het wantrouwen vanuit de overheid naar de burgers toe. Door overheden die zich opstelden als opponent van de burger die preventief beschouwd en behandeld werd als een potentieel crimineel risico element.

Hetgeen de overheid zich veelal ongestraft kon veroorloven omdat het voor de burger nagenoeg of geheel onmogelijk is gemaakt om zich tegen deze praktijk te verweren. Zoals blijkt uit de slepende uitputtende juridische procedures van burgers tegen onacceptabele inbreuken op hun privacy door de overheid. Waarbij, zoals in de rechtszaken die Vrijbit voerde duidelijk blijkt dat dit onvermogen zich ook uitstrekt tot de nationale rechtspraakinstanties om hier paal en perk aan te stellen.



Waarbij we voorzichtig optimistisch opmerkten dat Vrijbit in 2018 deze tendensen niet langer, samen met de Nationale Ombudsman, als ‘roepende in de woestijn’ signaleerden. Nu bleek dat instanties als de Raad voor de Rechtspraak, de Raad van State, de Vereniging voor Bestuursrecht (VAR) zich publiekelijk ook steeds vaker uitspraken over de democratie ondermijnende vertrouwenscrisis. Waarbij burgers omgekeerd evenredig aan het wantrouwen van de overheid ook steeds minder vertrouwen bleken te kunnen stellen op een solide wetgevende macht, en een effectief opererende rechterlijke macht.

In Jaarverslag van de Nationale Ombudsman lezen we *‘Het zijn al lang niet meer alleen de meest kwetsbaren die niet mee kunnen komen. Ook zelfredzame burgers lopen vast’* en *’diensten worden ook na de decentralisaties verder weg van de burger georganiseerd, loketten verdwijnen en het wordt steeds lastiger om een echt mens aan de lijn te krijgen. Efficiënt werken en goede verantwoording – beiden toch bedoeld om het beter te regelen voor de burger – keren zich zo juist tegen de burger.’*

In het jaarverslag van de Raad van State 2018 staat aldus expliciet aangegeven dat de wetgever zijn rol in de praktijk beter dient te vervullen: *‘De wetgever leunt steeds vaker en intensiever op andere partijen om tot wetgeving te komen. Dat is op zichzelf een begrijpelijke en positief te waarderen ontwikkeling. Maar er zijn wel grenzen aan. De wet mag niet louter een product zijn van een of meer groepen in de samenleving, of slechts een stempel zetten op akkoorden die*

maatschappelijke partners bereiken. Zij vertegenwoordigen niet het algemeen belang, maar brengen – om begrijpelijke en vaak valide redenen – een bijzonder belang naar voren, een deelbelang. Het gaat bij het algemeen belang niet alleen om een uitwisseling van deelbelangen of om wat een meerderheid afspreekt, maar ook om de beginselen van de democratische rechtsstaat. Daarin wordt rekening gehouden met de belangen en rechten van minderheden en individuen.'

We wijzen hier ook op berichten uit 2018 zoals die van 10 juni in de Telegraaf met als aanhef: '*Een forse groep mensen vindt de overheid eerder een vijand dan een bondgenoot.'* Of van de jaarvergadering van de Vereniging voor Bestuursrecht (VAR) op 18 mei. Waar verslag werd gedaan dat *'prof. mr. dr. Leo Damen (Hoogleraar Rijksuniversiteit Groningen), mr. Tijn Kortmann (verbonden aan de Universiteit Utrecht en advocatenkanoor Stibbe) en mr. Reinier van Zutphen (Nationale ombudsman) als expert adviseurs allen een toenemend gebrek aan vertrouwen in de overheid signaleerden en de noodzaak benadrukten om daar verandering in te brengen.'*

En op de harde feiten die aan het licht kwamen, zoals door het nieuwsbericht van AP op 15 februari 2018 dat gemeenten te veel persoonsgegevens verzamelden bij uitvoering Wmo en Jeugdwet'.

Onderstaand vermelden we ter illustratie ook een deel van de nieuwe wetten en wetsvoorstellen uit 2018 met dank aan de Privacybarometer:

Privacy Barometer
De actuele stand van de politiek over privacy

- - Inzet kentekenscanners door de belastingdienst
- - Flexibeler gebruik leerlinggegevens
- - Beschikbaar maken betaalgegevens bij banken
- - Uitvoeringswet AVG
- - Verruimen strafrechtelijke aanpak terrorisme
- - Gebruik risicoprofielen in de zorg krijgt wettelijke basis
- - Constitutionele toetsing
- - Wijziging wet DNA-verwantschapsonderzoek
- - EU plan verplichting vingerafdrukken in paspoorten ID
- - Wet bevorderen data uitwisseling voor samenwerkende instanties voor fraudebestrijding en rechtmatige zorg
- - Aanpassing bewaarplicht telecommunicatiegegevens

PrivacyNieuws.nl

Onderstaand overzicht van de door Vrijbit's Privacynieuwsdienst gepubliceerde digitale nieuwsbrieven geeft een overzicht van de veelheid en verscheidenheid aan wekelijkse berichten.

Het overzicht geeft links naar deze weekoverzichten. Berichten die op de website zelf niet alleen chronologisch, maar ook op onderwerp te doorzoeken zijn.

- Privacynieuws weekbrief - 52 Verzonden op 28 december 2018
- Privacynieuws weekbrief - 51 Verzonden op 21 december 2018
- Privacynieuws weekbrief - 50 Verzonden op 14 december 2018
- Privacynieuws weekbrief - 49 Verzonden op 07 december 2018
- Privacynieuws weekbrief - 48 Verzonden op 30 november 2018
- Privacynieuws weekbrief - 47 Verzonden op 23 november 2018
- Privacynieuws weekbrief - 46 Verzonden op 16 november 2018
- Privacynieuws weekbrief - 45 Verzonden op 10 november 2018
- Privacynieuws weekbrief - 44 Verzonden op 02 november 2018
- Privacynieuws weekbrief - 43 Verzonden op 26 oktober 2018
- Privacynieuws weekbrief - 42 Verzonden op 19 oktober 2018
- Privacynieuws weekbrief - 41 Verzonden op 12 oktober 2018
- Privacynieuws weekbrief - 40 Verzonden op 05 oktober 2018
- Privacynieuws weekbrief - 39 Verzonden op 28 september 2018
- Privacynieuws weekbrief - 38 Verzonden op 21 september 2018
- Privacynieuws weekbrief - 37 Verzonden op 14 september 2018
- Privacynieuws weekbrief - 36 Verzonden op 08 september 2018
- Privacynieuws weekbrief - 35 Verzonden op 01 september 2018
- Privacynieuws weekbrief - 34 Verzonden op 26 augustus 2018
- Privacynieuws weekbrief - 33 Verzonden op 17 augustus 2018
- Privacynieuws weekbrief - 32 Verzonden op 10 augustus 2018
- Privacynieuws weekbrief - 31 Verzonden op 04 augustus 2018
- Privacynieuws weekbrief - 30 Verzonden op 27 juli 2018
- Privacynieuws weekbrief - 29 Verzonden op 20 juli 2018
- Privacynieuws weekbrief - 28 Verzonden op 13 juli 2018
- Privacynieuws weekbrief - 27Verzonden op 06 juli 2018
- Privacynieuws weekbrief - 26 Verzonden op 29 juni 2018
- Privacynieuws weekbrief - 25 Verzonden op 22 juni 2018
- Privacynieuws weekbrief - 24 Verzonden op 15 juni 2018
- Privacynieuws weekbrief - 23 Verzonden op 08 juni 2018
- Privacynieuws weekbrief - 22 Verzonden op 01 juni 2018
- Privacynieuws weekbrief - 21 Verzonden op 25 mei 2018
- Privacynieuws weekbrief - 20 Verzonden op 18 mei 2018
- Privacynieuws weekbrief - 19 Verzonden op 12 mei 2018
- Privacynieuws weekbrief - 18 Verzonden op 04 mei 2018
- Privacynieuws weekbrief - 17 Verzonden op 27 april 2018
- Privacynieuws weekbrief - 16 Verzonden op 20 april 2018
- Privacynieuws weekbrief - 15 Verzonden op 13 april 2018
- Privacynieuws weekbrief - 14 Verzonden op 06 april 2018
- Privacynieuws weekbrief - 13 Verzonden op 31 maart 2018
- Privacynieuws weekbrief - 12 Verzonden op 23 maart 2018
- Privacynieuws weekbrief - 11 Verzonden op 16 maart 2018
- Privacynieuws weekbrief - 10 Verzonden op 09 maart 2018
- Privacynieuws weekbrief - 9 Verzonden op 02 maart 2018
- Privacynieuws weekbrief - 8 Verzonden op 23 februari 2018
- Privacynieuws weekbrief - 7 Verzonden op 17 februari 2018
- Privacynieuws weekbrief - 6 Verzonden op 09 februari 2018

- Privacynieuws weekbrief - 5 Verzonden op 02 februari 2018
- Privacynieuws weekbrief - 4 Verzonden op 26 januari 2018
- Privacynieuws weekbrief - 3 Verzonden op 19 januari 2018
- Privacynieuws weekbrief - 2 Verzonden op 13 januari 2018
- Privacynieuws weekbrief - 1 Verzonden op 05 januari 2018

Actuele en doorlopende kwesties



De door Vrijbit al in 2011 gepresenteerde '5 Principes van Privacy Preventie' als denkraam om het alom aanwezige fenomeen van privacybedreigingen behapbaar te maken voldoen daar onverminderd toe. Onderstaand geven we aan de hand van deze 5 punten een aantal voorbeelden van zaken die in 2018 op de voorgrond sprongen.

Waar bevindt een persoon zich, en heeft hij zich bevonden?

Automatic Number Plate Registration (ANPR) met aan de ene kant de politie en Belastingdienst die blijven inzetten op het gebruik van kentekenregistratie voor ruimer gebruik dan voor de opsporing en beboeten van verkeersovertredingen. Met anderzijds burgers die juridische procedures voeren tegen het langdurig bewaren van kentekengegevens en gebruik voor controle op andere zaken.

'Connected cars. Zorgen over de ontwikkeling dat auto's steeds meer data verzamelen over de activiteiten van de bestuurder. Gegevens over onder meer de locatie, de technische staat van de auto en het verbruik verzonden naar de autofabrikant de ontwikkelaar van de connector/dongel of naar de 112-centrale. Met zorgen over het gebruik dat van de data kan worden gemaakt voor allerlei producten en diensten, zoals e-Call (automatische oproep hulpdiensten bij een ongeval) het analyseren van rijgedrag van de bestuurder (die daarop tips kan krijgen om zuiniger of veiliger te rijden). Locatiegegevens voor gebruik van marketing. Doorgifte van technische en operationele data naar de fabrikant waarmee deze automatisch ook de beschikking krijgt over (bijvoorbeeld locatie)gegevens waar men niets mee nodig heeft. De zorgen over de gevolgen in geval van hacking en hoe de juridische aansprakelijkheid te regelen bij ongelukken met zelfrijdende

voertuigen. Bezwaren ook tegen de opzet van de EU om e-Call in nieuwe personenauto's verplicht te stellen waarmee automobilisten geen keus meer hebben om zich anoniem per auto te verplaatsen(en hoe dit zich verhoudt tot de verplichte toestemmingsregels uit de nieuwe EU General Data Protection Regulation (EU wet bescherming persoonsgegevens GDPR).

Betaald parkeren. Met aanhoudend rechtszaken tegen de koppeling van parkeerbelasting aan kentekenregistraties en elektronische betaaldiensten.

Dat zijn alleen al drie voorbeelden van actuele kwesties in zake automobilisten-registratie.

Vliegtuigpassagiers. Met betrekking tot het vastleggen van het luchtverkeer noemen we het wetsvoorstel (toelichting) van minister Grapperhaus (CDA) om gegevens van vliegtuigpassagiers binnen Europa voor de opsporing te gaan gebruiken. Waarbij de gezochte verdachten (van zware misdrijven t/m fraude, valsheid in geschrifte, computercriminaliteit, witwassen, milieu-misdrijven en illegale kunsthandel). En software programma's tevens middels geheime zoekopdrachten risicoprofielen samenstellen van mensen die aan de hand van bepaalde combinaties van gegevens als verdacht worden aangemerkt.

Dit wetsvoorstel is een schoolvoorbeeld van hoe de Nederlandse regering een verregaande privacyaantasting probeert door te voeren waarbij iedereen die zich met een vliegtuig verplaatste het risico loopt om totaal onschuldig toch als (terrorisme) verdachte terecht te kunnen komen in opsporingssystemen. De tactiek hierbij is om in eerste instantie de verplichte NPR vanuit de EU inzake intercontinentale vluchten niet om te zetten in nationale wetgeving. Om vervolgens het parlement, tegen de adviezen van o.a. de Raad van State in toch als de donder met de nationaal 'opgetopte' wet te laten instemmen omdat de EU een boete van 3,7 miljoen dreigt te gaan opleggen omdat de verplichte EU PNR niet op tijd is geïmplementeerd. *Deze strategie van omzeilen van democratische besluitvorming en de EU de schuld geven kennen we al van de Paspoortwet in 2006 en 2009 en van de Wet Bewaarplicht Telecommunicatie gegevens.*

Locatiegegevens. De i-Phone vormde in 2018 de spin in het web van het internetgebruik in Nederland. Steeds meer mensen gebruikten ook steeds intensiever de tablet-pc (i-PAD). De apparaten legden, zonder dat de meeste gebruikers zich ervan bewust zijn dat de provider gemiddeld om de 15 minuten 24 uur per dag de locatiegegevens opslaat, daarmee vrijwel continu vast waar het apparaat en de gebruiker zich bevinden. Dit is uiterst waardevolle informatie voor de internet bedrijven en hun adverteerders. Dat geldt des te meer voor het vastleggen van de locatiegeschiedenis, waarmee van miljoenen gebruikers zowel tot in detail kan worden bijgehouden wanneer zij zich waar bevinden als volgens welk patroon zij hun leven leiden. Het vastleggen voor gerichte reclame doeleinden vinden sommige mensen positief. Anderen ervaren het als inbreuk op hun privacy. Voor sommige doeleinden is de techniek van GPS, WiFi en Bluetooth prima of zelfs onontbeerlijk. Maar er zijn ook toepassingen die helemaal niet in het belang van de gebruiker zijn. Het inperken van de privacy aantasting door locatieregistratie, vergt moeite en technische kennis. Daardoor blijken zelfs diegenen die zich wel bewust zijn van de bezwaren en gevaren, nauwelijks gemotiveerd om daadwerkelijk alle instellingen op hun apparaat hierop aan te passen. Ook niet met behulp van de 'toolbox' die Bits of Freedom hiervoor beschikbaar stelt via hun website.

Cameratoezicht door bedrijven en particulieren voor het beveiligen van hun panden en goederen nam steeds meer toe. Hetgeen ook gold voor het uitdijen van de database 'Camera in Beeld' van de politie om hier intensief gebruik van te maken. Verder diende we er in 2018 ook aan te wennen dat men in de publieke ruimte ook als onverdacht persoon door de politie met camera's

in beeld kan worden gebracht via mobiele surveillancecamera's en via drones(zoals tijdens Oud- en Nieuw in Utrecht).

De AIVD en MIVD mogen sinds mei 2018 ook zonder notificatie en zonder tussenkomst van een rechter of officier van justitie inloggen op computers van zowel verdachten als van personen die zelf geen target van de inlichtingendiensten zijn. Waarmee iedereen die gebruik maakt van een computer met cameraoptie ongemerkt gefilmd kan worden.

En tot slot maar niet als minste voorbeeld geldt natuurlijk de nauwelijks te beteugelen drift van velen particulieren om foto's en filmpjes te maken met hun i-Phone of i-Pad en deze beelden, ook als daar ongevraagd mensen mee worden vastgelegd via internet aan anderen te sturen of voor openbaar gebruik te publiceren.

Waarmee we direct raken aan een van de hoofdthema's waar Vrijbit zich mee bezig houdt, namelijk de nog almaar toenemende technische mogelijkheden van biometrische identificatie via gezichtsherkenning.

Met wie heeft de persoon contact en waar haalt hij of zij informatie vandaan.

Ook hier is de meest in het ooglopende kwestie van 2018 dat, door het van kracht worden van de Wiv-2017 de nationale inlichtingen- en veiligheidsdiensten zonder tussenkomst van een rechter eigenstandig per sleepnet alle telecommunicatie die via de kabel verloopt als bulk data kunnen binnenslepen. Ook de communicatie en het website bezoek van personen en groepen die op geen enkele manier als verdacht gelden, maar daarmee wel onderworpen raken aan de realiteit dat men niet weet of men in vrijheid kan functioneren zonder door AIVD-MIVD in de gaten te worden gehouden. Een impact volgens het 'Panopticon' principe dat mensen ertoe worden aangezet om zich terughoudend te gedragen bij de wetenschap dat men wellicht door derden bespioneerd wordt. Een verregaande privacyaantasting derhalve die in ernst nog overtroffen wordt door de bevoegdheden in de Wiv dat de geheime diensten, zelfs als men deze bulkdata niet zelf heeft bekeken/geanalyseerd, mag delen met buitenlandse geheime diensten(waardoor iedere regie op wat deze diensten vervolgens met deze data doen uit handen wordt gegeven).

Hoe komt de persoon aan inkomsten en hoe besteedt hij deze?



Met name de inperking van de mogelijkheden tot contante betaling zijn van belang om alle geldstromen via elektronische weg te kunnen registreren en controleren. Waarbij in 2018 de overheid flink heeft moeten inbinden in haar streven om een cashloze samenleving te bewerkstelligen door het verbod voor gemeentes om contante betalingen onmogelijk te maken. Hoewel dit niet uit privacyaspecten gebeurde was de bescherming van het anoniem kunnen betalen wel het resultaat.

22-10-2018 Kennisgeving Binnenlands Bestuur:De Europese Centrale Bank (ECB) tikt gemeenten op de vingers waar burgers aan de balie niet meer met contant geld kunnen betalen. Volgens Europees recht is een pin-only beleid niet geoorloofd.

De ECB heeft dat de Vereniging van Nederlandse Gemeenten (VNG), via De Nederlandsche Bank (DNB), laten weten. Burgers moeten aan de gemeentelijke balie contant kunnen betalen, zonder daarvoor bijzondere redenen aan te voeren.

De lichamelijke gesteldheid

De jacht op ieders medische gegevens was in volle gang! Waar 'Big data' inmiddels alom werden beschouwd als het nieuwe goud van de wereldwijde economie, stonden medische gegevens daarbij met stip als de meest waardevolle persoonsgegevens te boek. Verzekeraars, wetenschappers, farmaceutische bedrijven, data-analisten, fabrikanten van medische apparatuur, gezondheids- apparaten, medische hulpmiddelen en internet applicaties, allemaal stonden ze te trappelen om zoveel mogelijk medische data ter beschikking te krijgen. Dat gold evenzeer voor de spelers op gebied van de ontwikkeling van Kunstmatige Intelligentie(AI) als partijen op gebied van robotisering. En niet te vergeten ook partijen die zich op een of andere wijze met voeding bezig houden.



Alle mogelijke bedrijven in binnen- en buitenland aasden op het verzamelen en vermarkten van zoveel mogelijk gegevens in zake gezondheid. Via enquêtes, draagbare apparatuur om lichaamsfuncties te meten, online gezondheids platformen en social media en commerciële DNA tests werd de informatiehonger gevoed.

e-Health was het toverwoord en als aanjager fungeerde de framing dat 'een integrale persoonsgerichte digitale zorgomgeving de patiënt en zijn zorg-netwerk in staat stelt zijn gezondheid en ziekte te managen'. *(citaat uit het interview e-Health Hype, revolutie of evolutie? d.d. 27-9-2018 ter beschrijving van het gezamenlijk streven van de acht UMC's in het programma e-Health) Bron: https://www.nfu-ehealth.nl/documenten/interview_vg_4-18_3p3.pdf*

De Nederlandse overheid liet zich in deze ook niet onbetuigd en leverde volop haar bijdrage aan de jacht op de medische gegevens van de Nederlandse inwoners. Onder het motto dat de marktwerking moet worden gestimuleerd wil de Zorg niet onbetaalbaar worden, zette de overheid in op het almaar intensiever verzamelen en verwerken van zo veel mogelijk medische gegevens. Zo mocht de Nederlandse Zorg autoriteit (NZa) ondanks het ontbreken van een wettelijke grondslag en tegen rechterlijke uitspraak over dit DIS systeem in, doorgaan met het periodiek ophalen van alle verplicht aan te leveren diagnose en behandel- combinatie gegevens (DBC's) uit de medisch-specialistische zorg. Werd geëist dat via de stichting Benchmark uiterst gedetailleerde patiëntgegevens uit de GGZ ter beschikking werden gesteld. Kregen de Zorgverzekeraars volop steun van de minister om met doorbreking van het medisch beroepsgeheim zonder toestemming van de betrokkenen zich rechtstreeks toegang te verschaffen tot patiëntgegevens ter controle van de medische hulpverleningspraktijk.(een wetsvoorstel wat uiteindelijk op het nippertje eind 2018 door de Eerste Kamer alsnog werd getorpedeerd).

Hoe is de persoon te koppelen aan zijn gegevens en aan zijn reeds opgeslagen data/gedragsprofiel?

Zoals eerder in dit jaarverslag aangegeven is er inmiddels erkenning gekomen voor het feit dat allerhande data over een persoon, die los van elkaar niet tot een persoon te herleiden zijn, in combinatie een zeer gedetailleerd beeld kunnen geven over een bepaalde persoon. Zo gedetailleerd dat er niet alleen een profiel gemaakt kan worden van de gedragingen van deze persoon, maar ook van de patronen volgens welke deze zijn of haar leven inricht. Gegevens die,zoals bleek uit onderzoeken van mensen die hun eigen digitale sporen probeerden te achterhalen, meer van een persoon bleken te weten dan dat de betrokkene zichzelf herinnerde of van bewust was. Gegevens die vrij nauwkeurig ook informatie opleverden over iemands te verwachten toekomstige gedrag.

Data die bij gevolg niet enkel van grote waarde werden geacht voor opsporings- en inlichtingendiensten, maar ook voor beleidsmakers en commerciële partijen.

Het aantal data wat hiervoor de grondstof leverde, groeide explosief. De drie grote leveranciers vormden ten eerste de mensen zelf. Ten tweede de particuliere commerciële bedrijven. En ten derde de overheidsdiensten. Dit gebeurde voor goed begrip niet los van elkaar, maar in een zodanig nauw verweven samenspel dat de verschillende aanlever-stromen nauwelijks van elkaar te onderscheiden waren.

Mensen maken immers gebruik van digitale apparaten onder gebruiksvoorwaarden van fabrikanten, Informatie en Communicatie Technologie(ICT) -en internetbedrijven. Overheden gebruiken die data die over mensen wordt geregistreerd,maar verplichten ook op allerlei gebied dat deze data afgegeven moeten worden. Ook via het gebruik van betaaldiensten worden data rechtstreeks gedeeld met overheidsdiensten *(hetzij rechtstreeks via hun persoon dan wel via de betaalgegevens van bedrijven waar elektronische betalingen worden gedaan).*

Dat mensen daar weinig tegen opkomen, uit onkunde of gemaksoverwegingen was niets nieuws.

Wel nieuw was het gegeven dat de overheid via de Wiv de inlichtingen- en veiligheidsdiensten ongekende nieuwe bevoegdheden gaf om data, zonder tussenkomst van een rechterlijk bevel, rechtstreeks 24/7 te onttrekken aan instellingen of bedrijven(1), met een sleepnet van grote groepen mensen alle telecommunicatieverkeer af te tappen(2) EN om via digitale apparaten van onverdachte personen inlichtingen te verzamelen over mensen die wel doelwit van de diensten vormden(3).

Ook nieuw was het effect van het op 25 mei 2018 van kracht worden van de nieuwe Algemene Verordening Gegevensbescherming. Wetgeving die de oude wet Bescherming Persoonsgegevens verving. Met als voordeel voor de privacy van burgers, dat binnen allerhande instellingen en bedrijven, noodgedwongen begon door te dringen dat iedereen zich aan de regelgeving ter bescherming van persoonsgegevens diende te houden. *Al dient daarbij opgemerkt dat veel van die regelgeving helemaal niet nieuw was, en ook onder de Wbp had dienen te worden nageleefd. Dat het belang van privacybescherming onder de AVG ineens wel opportuun werd, had vooral te maken met het feit dat er voortaan door AP (hoge)boetes konden worden uitgedeeld aan wie zich niet aan de wet hield.* Daarnaast luidde deze nieuwe wetgeving ook een nieuw tijdperk in voor de overheid, die zich op grond van de EU uitzondering ‘ De verordening is niet bedoeld om van toepassing te zijn op de verwerking van persoonsgegevens voor activiteiten op het gebied van nationale veiligheid of rechtshandhaving in de EU’ juist meende nog veel ruimer gebruik te

kunnen maken van de mogelijkheden om persoonsgegevens te kunnen opeisen en gebruiken van onschuldige burgers. Waarvan de poging om naast het verfoeide SYRi systeem, ter screening van onverdachte personen als potentiële fraudeurs, een Kaderwetsvoorstel werd gelanceerd voor data uitwisseling door samenwerkende ketens voor fraudebestrijding/rechtmatige zorg (34972*) Door Vrijbit als werktitel aangeduid als 'wet overheid mag alles' of' SYRi-02'.* Door de overheid gepresenteerd als 'Algemene regels inzake het elektronisch verkeer in het publieke domein en de generieke digitale infrastructuur (Wet digitale overheid)'Bron: 7- 6-2018 https://www.internetconsultatie.nl/rechtmatigezorg Een wetsvoorstel dat beoogd het net van totalitaire surveillance van iedere inwoner van Nederland nog verder te sluiten.

Tot slot

De vermelding van de nieuwe pogingen in 2018 van de Europese Commissie om alsnog de vingerafdrukken in de ID-kaarten te gaan verplichten. Vreselijk nieuws gezien de strijd die Vrijbit al meer dan 10 jaar voert tegen de biometrische paspoorten en ID-kaarten. Tekenend voor de overmacht waartegen een burger te hoop loopt als hij gebruik wil maken van het rechtssysteem om tegen de overheid in opstand te komen als deze op onacceptabele wijze zich iemands biometrische kenmerken wil toe-eigenen.

Immers waar deze strijd vooralsnog deels positief resulteerde in het 5 jaar geleden afschaffen van de vingerafdrukken in de Nederlandse ID-kaart wordt dit via de Ubocht van EUpolitiek alsnog weer als verplichting voor de Nederlandse overheid georganiseerd. *Waarmee de uitspraak van de Raad van State dat de vingerafdrukweigeraars in het gelijk werden gesteld bij herinvoering via deze route geen werking meer heeft. Omdat de Nederlandse rechter zorgvuldig vermeed een principiële uitspraak te doen en enkel inging op de onterechte stelling van de Nederlandse overheid dat de vingerafdruk in de ID-kaart door Europa werd verplicht.* Dit alles terwijl de juridische strijd tegen de vingerafdrukken in de paspoorten en de digitale gezichtsopname in paspoort en ID-kaarten werd voortgezet bij het Europese Hof voor de Rechten van de Mens, die de zaak al jaren op de plank laat liggen.

Activiteiten van Vrijbit in 2018



Hoofddossiers

De belangrijkste dossiers waar Vrijbit zich in 2018 mee heeft bezig gehouden betroffen:

De jacht op onze medische gegevens.

Met name de **onrechtmatige aanmeldingen in het EPD-LSP** die leidde tot 2 bezwaarprocedures die onze vereniging aanspande tegen de Autoriteit Persoonsgegevens, omdat deze toezichthouder weigerde in te grijpen bij de beheerder van het systeem noch bij de apothekers die systematisch onrechtmatig mensen in het systeem aanmeldden. bezwaarprocedures die uitmondden in het opstarten van 2 beroepszaken hierover bij de rechtbank Midden-Nederland



gebouw VZVZ beheerder EPD-LSP systeem, Oude Middenweg 55
2491 AC Den Haag

Het **Whitebox alternatief voor EPD-LSP** werd na jaren vooronderzoek in april eindelijk door de huisartsenposten in Amsterdam in gebruik genomen. De ontwikkeling van deze 'Whitebox' technologie, een alternatief 'privacy-proof' uitwisselingssysteem voor medische gegevens, heeft Vrijbit van meet af aan actief gesteund door er op allerlei manieren bekendheid aan te geven.
Voor meer informatie zie de publicatie 04-04-2018: Privacyvriendelijk alternatief EPD officieel in gebruik genomen https://platformburgerrechten.nl/2018/04/04/privacyvriendelijk-alternatief-epd-officieel-in-gebruik-genomen/

Nederlandse Zorgautoriteit

De voortzetting van de queeste over het **Diagnose Informatie Systeem DIS van Nza**. Een kwestie die sinds 3-5-2015 door Vrijbit aanhangig is gemaakt en zich na uitputtende bezwaar- en beroepsprocedures inmiddels alweer jaren voortsleept bij de Rechtbank Midden-Nederland als dossier UTR 16/4199

WBP V93, *wegens tegenwerking van AP, NZa en het ministerie*, en waarin nog steeds geen definitieve uitspraak in eerste aanleg is gedaan. Als tussen-succesje valt te melden dat de Nza al wel heeft moeten stoppen met het doorgeven van de medische herleidbare patiëntdata uit het DIS aan diverse derde partijen, en in november 2018 aankondigde minder data voor het DIS te gaan opeisen. Maar fundamenteel is dit geen bevredigende oplossing voor het DIS systeem waarbij onrechtmatig tot de persoon herleidbare data via het DIS voor 'beleidsdoeleinden' worden verzameld en verwerkt.(2). Dat de zaak na 'nadere inbreng' van *(grotendeels zwartgemaakte, geheime)*processtukken door AP opnieuw op zitting zou komen, werd aangekondigd voor 15 februari 2019.

De voortgang van de **rechtszaak tegen de Gedragscode van de Zorgverzekeraars** (UTR 16/3326 WBP V97) om reden dat deze particuliere bedrijven in strijd handelen met nationaal-en internationaal recht ter bescherming van de privacy en het medisch beroepsgeheim. Eveneens een zaak die speelt sinds mei 2015 omdat de AP niet wenste in te grijpen en de verzekeraars de handen boven het hoofd bleef houden om de bestaande praktijk *(van georganiseerde onverantwoordelijkheid)* te laten voortduren. Met als enige aanpassing dat AP aan de vier grote verzekeraars opdracht had gegeven om betere waarborgen in hun werkprocessen in te bouwen om het gebruik van patiëntgegevens door hun commerciële marketing afdelingen te beëindigen. Zorgverzekeraars Nederland, de belangenvereniging onder wiens leiding de Gedragscode bij alle verzekeraars als informatie naar de klanten wordt gepubliceerd over hoe er met hun gegevens wordt omgegaan is in de hele procedure door AP buiten schot gelaten.

Actie Stop Rom (Routine Outcome Monitoring) Vrijbit steunde de actie van de Stichting Stop Benchmarking GGZ om de privacyaantastende verzameling van een uiterst gedetailleerd pakket aan persoonsgegevens van mensen in de GGZ te moeten aanleveren aan de stichting Benchmarking GGZ. ROM-data bovendien totaal niet geschikt zijn voor de kwaliteitsdoeleinden, benchmarking en zorginkoop waar ze voor bedoeld zijn.

Net als de acties waar Vrijbit zelf het voortouw toe nam, gaat het hier om een taai gevecht. Zo passeerden begin 2018 een schijnoplossing waarbij het aanleveren van data door vrijgevestigde hulpverleners niet meer bij voorbaat werd 'aangezet', maar ze vervolgens zelf de verantwoordelijkheid kregen om al dan niet hun bulk data te leveren terwijl ROM data bij wet enkel mogen worden verstrekt wanneer de betrokken cliënt daar expliciet toestemming voor heeft gegeven. Heel 2018 werd er geprobeerd om via discussie binnen de GGZ en de politiek een eind te maken aan het Rommen. Waarbij eind 2018 de stand van zaken was dat de stichting Benchmark opging in een nieuwe alliantie AKWA waar de gegevens nu zouden moeten worden aangeleverd voor onderwijsdoeleinden. Intussen liep er nog steeds een handhavingsverzoek bij AP om een eind aan de privacyinbreuken te maken en werd er een tuchtrechtprocedure door patiënten/cliëntenbetreffende de ROMproblematiek voorbereid tegen de grote GGZ instellingen.

Actie (Ont)Regel de Zorg. Een actieve beweging gestart door Actiecomité Het Roer Moet Om en VvAA (collectief van ruim 123.000 zorgverleners) heeft als doel om de zorg te ontdoen van

overbodige bureaucratie. Zodat er meer tijd ontstaat voor de patiënt en meer werkplezier voor de zorgverlener. Ook dit is een beweging waar Vrijbit zich waar het maar kan voor inzet om de link te leggen tussen de administratieve regeldrift en het daarmee in het geding zijnde aspect van privacy.

Tot slot nog de vermelding dat Vrijbit zich tot het uiterste heeft ingespannen om **de geheime DNA databank** als aspect van de nieuwe Wiv onder de aandacht van het grote publiek te brengen. Met enig succes getuige de publicatie van onderstaande publicaties:



Vrijbit home website: https://www.vrijbit.nl/dossiers/veiligheids-en-inlichtingendiensten/item/1084-de-geheime-dna-databank,-als-onderbelicht-aspect-van-de-nieuwe-wiv-toegelicht.html

De Groene Amsterdammer, 'De DNA-verzameldienst' https://www.groene.nl/artikel/de-dna-verzameldienst

NRC 20-3-2018 Sleepwet zet 25 jaar DNA-strafwetgeving bij oud vuil https://www.nrc.nl/nieuws/2018/03/20/sleepwet-zet-25-jaar-dna-strafwetgeving-bij-oud-vuil-twee-regels-a1596375

> Zelfs de artsenfederatie KNMG werd door leden van Vrijbit zodanig opgepord dat men daar begon te beseffen dat de WIV ook hen als professionals aanging door dat AIVD toegang ging krijgen om 'in bulk' privacygevoelige gezondheidsgegevens te verzamelen te gebruiken en te delen(met buitenlandse inlichtingendiensten). *Al liet deze organisatie zich na een kniebuiging van de AIVD met een publicatie dat er echt heus nooit ongericht van deze bevoegdheden gebruik zou worden gemaakt, weer geruststellen.*

Daarnaast steunde Vrijbit, met raad en daad, eveneens personen en organisaties die zich verzetten tegen de oprukkende aantasting van de privacy van patiënten en het medisch beroepsgeheim vanuit andere hoek.

Waarbij met name de ontwikkeling van nieuwe wetgeving inzake de elektronische uitwisseling van patiëntgegevens/gezondheidsdata die ten doel hebben om zorgverzekeraars de bevoegdheid te geven om zich rechtstreeks toegang te verschaffen tot medische dossiers bij de hulpverleners voor preventief fraudeonderzoek en zogenaamde materiële controle. *NB Waarbij onder 'materiële controle' verstaan dient te worden dat het gaat over toezicht op de individuele zorgverlening volgens de criteria die de verzekering stelt ten aanzien van de duur en inhoud van medische behandelingen en door wie en waar deze volgens voorschrift van hen mogen plaatsvinden.* Een wetvoorstel wat op 18 december 2018 uiteindelijk na veel tegenactie door de Eerste Kamer werd verworpen.

De nieuwe wet op de inlichtingen- en veiligheidsdiensten(Wiv-2017)







Vrijbitleden hebben in 2018 letterlijk stad en land afgereisd om het referendum tot een succes te maken. Dat lukte dankzij het verspreiden van een gigantische stroom informatie, waar onze organisatie een aandeel in had om de daadwerkelijke inhoud van het wetsvoorstel te verduidelijken en misvattingen daarover uit de weg te ruimen. En om tijdens de honderden bijeenkomsten en acties toelichting te geven op de informatie en vragen die mensen daarover hadden. We namen deel aan tientallen debatten, organiseerden er zelf meerdere, verspreiden nieuwe stickers die opriepen om toch vooral te gaan stemmen en steunden andere actievelingen (waaronder de initiatiefnemers van het referendum) met raad en raad.



Intussen waren we betrokken bij de voorbereidingen van een civiele procedure tegen de Wiv en onderzochten met behulp van Piper advocaten de mogelijkheid om rechtstreeks naar het EHRM te stappen vanwege de onomkeerbare schade die aangericht kon worden met invoering van de Wiv.

Uiteindelijk werd de wet toch van kracht in mei 2018, al had intussen de Tweede Kamer wel afgedwongen dat evaluatie van de wet eerder zou plaatshebben dan gepland en dat er aanpassingen zouden worden gemaakt op de uitwisseling van ongeanalyseerde data aan buitenlandse diensten. Als laatste statement hebben we toen aan de (nieuwe toezichtcommissie op de nieuwe bevoegdheden van de AIVD-MIVD *(let op niet op de uitgebreide!!)* de TIB een stempel aangeboden met de tekst ‘Tegen de Mensenrechten’ en een stempel kussen met rode inkt.

Stand van zaken eind 2018 was dat zowel de TIB als de Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten(CTIVD)zelf concludeerden dat de inzet van de bevoegdheden niet op orde was. De TIB dat er geen toestemming diende te worden gegeven in veel verzoeken om het sleepnet voor ondervanging van telecommunicatieverkeer in te zetten omdat dit onevenredig de

privacy zou schaden, de CTIVD omdat de dienst haar eigen richtlijnen voor naleving van de randvoorwaarden van de Wiv niet op orde had.

De omzetting van de Wet Bescherming Persoonsgegevens(Wbp) naar de Algemene Verordening Gegevensbescherming(AVG).



Nadat de EU de databeschermingsrichtlijn uit 1995, als verouderd werd beschouwd, werd jarenlang gewerkt aan de opzet van een nieuw framework voor dataprotectie wat beter op de moderne digitale tijd zou zijn toegesneden. Aan die oorspronkelijke opzet heeft Vrijbit actief deelgehad. Na jaren lobby van bedrijven en overheden om deze opzet af te zwakken werd uiteindelijk de nieuwe General Data Protection Regulation (GDPR) EU 2016/679 aangenomen. Dit is een Europese Verordening (dus met rechtstreekse werking) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.

Nederland kreeg tot 25 mei 2018 de tijd om deze EU wetgeving verplicht om te zetten in nationale wetgeving. Daarmee verdween op die datum de wet Bescherming Persoonsgegevens en werd deze vervangen door een Algemene Verordening Persoonsgegevens(AVG). Dat had nogal wat voeten in aarde omdat er vlak tevoren ineens in allerlei instanties, verenigingen en bedrijven een soort AGV paniek uitbrak omdat het nu toch echt menis bleek te zijn met de dreiging dat als men zich niet aan de bepalingen uit de AVG zou houden daar fikse boetes voor konden worden uitgedeeld door de Autoriteit Persoonsgegevens(AP).

Dat had tot gevolg dat er naast een broodnodige bewustwording in bijvoorbeeld het onderwijs, ten aanzien van de omgang met leerling-gegevens ook allerlei indianenverhalen de ronde gingen doen.

Met bijvoorbeeld kerkgenootschappen die aan de bel trokken omdat men dacht dat de AVG zou verbieden om in de kerk voor zieke parochianen te bidden of de namen van overledenen af te kondigen. Er was, om nog maar eens zo'n doorgeschoten voorbeeld te noemen, ook een huisarts die de landelijke pers haalde omdat hij- totaal bezijden de waarheid- berichtte dat hij nu geen

patiëntgegevens meer mocht uitwisselen met andere bij een bepaalde behandeling van zijn patiënten betrokken artsen. Zelfs de meldplicht datalekken, die vooruitlopend op de wet al van kracht was geworden, leidde tot misverstanden zoals bleek tijdens een lezing op de nationale onderwijsbeurs waar glashard gesteld werd dat als iemand intern een datalek had ontdekt en dat snel had verholpen dit als incident niet gemeld zou hoeven te worden. Ook met betrekking tot het begrip uit de wet 'the right to be forgotten' bleek keer op keer dat onbekend was dat dit slechts betrekking had op de mogelijkheid data door de bedrijven van internet zoekmachines niet publiekelijk vindbaar te maken.

Vrijbit heeft derhalve bij allerlei gelegenheden tegengas moeten geven aan de overtrokken aanduidingen van de AVG door de overheid, toezichthouder en de media dat 'Door de AVG de privacyrechten van mensen versterkt en uitgebreid zijn'. Dit met name omdat veel bepalingen ook onder de oude wet allang dienden te worden nageleefd. En ook omdat de wet niet (dan wel maar heel beperkt) toeziet op hoe overheden persoonsgegevens moeten beschermen.

> Citaat uit Brief Vrijbit aan rechtbank Midden Nederland sector bestuursrecht (UTR 16/3326 WBP V97) 10-4-2018
>
> *Mogelijk ten overvloede willen wij er hier nogmaals op wijzen dat ook met het inwerking treden van de Algemene Verordening Gegevensbescherming (AVG) d.d.25-05-2018 de verwerking van medische persoonsgegevens op basis van een wettelijke grondslag nog steeds vereist dat voldaan wordt aan de vereisten van voorzienbaarheid (van extra belang waar het hier gaat om een inbreuk op een fundamenteel burgerrecht) en doelbinding. Dit laatste zoals eerder opgemerkt ook om relevante toetsing aan de kernbeginselen van het privacyrecht mogelijk te maken.*
>
> *Het is zeer pijnlijk te moeten constateren dat de benadering die ten grondslag ligt aan de nieuwe beslissing op bezwaar van de toezichthouder feitelijk neerkomt op het erkennen en laten voortbestaan van een conditie van georganiseerde onverantwoordelijkheid. Dit is uiterst schadelijk voor het vertrouwen dat burgers zouden moeten kunnen stellen in een onafhankelijk publiek toezicht op de bescherming van hun fundamentele recht op bescherming van het privéleven, en dat van hun medische persoonsgegevens in het bijzonder. Ook voor een goed functionerende rechtstaat, en het vertrouwen wat burgers daarin moeten kunnen stellen is het desastreus als instanties/bedrijven deze persoonsgegevens ongestraft op onrechtmatige wijze kunnen verwerken en de daartoe ingestelde toezichthouder hen daarbij faciliteert in plaats van terecht wijst.*

Ook het feit dat er zo hoog werd opgegeven van het feit dat allerlei organisaties in bepaalde situaties nu verplicht waren om een functionaris gegevensbescherming (FG) aan te stellen die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG). Een voorschrift waarvan gedaan wordt alsof dat automatisch tot een betere privacybescherming zou leiden, maar die net zo goed negatief kan uitwerken. Bijvoorbeeld omdat er geen criteria zijn voor waar zo'n functionaris aan moet voldoen en omdat de geschiedenis ons leerde dat (zoals in onze zaak tegen de NS) FG-ers die (wel) deskundig zijn ook bij uitstek kunnen functioneren om voor hun werkgever de mazen van de wet te kennen.

Wel waren we weer enthousiast over het feit dat de AP nu verplicht is om klachten die individuen indienen in behandeling te nemen. Het gehalte van deze behandeling stellen we ons, gezien onze ervaringen met AP en de leegloop aan deskundig personeel in 2018, maar niet teveel van voor. Maar het maakte in elk geval een einde aan het beleid van augustus 2015 waarbij individuele

klachten niet langer voor behandeling in aanmerking kwamen. Dit naar aanleiding van de actie van ons Meldpunt Misbruik ID-plicht bij de massale klachten over de onjuiste her-identificatieplicht van banken het (toenmalige) College bescherming persoonsgegevens in te schakelen.

Hoe het in de praktijk ook moge uitwerken, feit is dat in 2018 de AVG een prettige bron van inkomsten heeft opgeleverd aan een legioen aan FG-ers, juristen en adviesbureau's die de AVG vooral als gat in de markt hebben ontdekt.

Paspoort –en ID-kaartzaken

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Omdat we nog steeds zaten te wachten op de behandeling van de zaken aangaande de vingerafdrukken in de paspoorten, de digitale gezichtsscan in paspoort en ID-kaart en de opslag van de persoonsgegevens in de documenten op een op afstand uitleesbare RFID-chip, stond ons niet veel anders te doen dan nauwgezet alle relevante ontwikkelingen met betrekking tot deze zaken te volgen en te documenteren. Daarbij ging het met name om de vlucht die de digitale gezichtsherkenningstechniek en toepassing daarvan heeft genomen. Om de politieke ontwikkelingen in de EU om vingerafdrukken in de nationale ID-kaart te gaan verplichten. En om de mondiale strijd om het eigendom van de chiptechnologie en mogelijkheden tot inbouw van 'achterdeurtjes' in de beveiliging daarvan.

Er zijn in Straatsburg, bij het hoogste mensenrechten Hof van de Raad van Europa, het EHRM, over deze kwesties vanuit Nederland 6 zaken aanhangig gemaakt. Vier paspoortzaken en 2 ID-kaart zaken. Juridische procedures die door particulieren werden aangespannen, waaronder 5 van leden van Vrijbit. Vrijbit coördineerde tijdens de nationale rechtsgang deze zaken, maar ziet zich nu net als de betrokkenen zelf geconfronteerd met de akelige situatie dat men het Hof niet mag benaderen om vaart achter de behandeling te gaan zetten, noch om in dit stadium aanvullende informatie te sturen. Een situatie die de tanden sowieso al deed knarsen. Extra pijnlijk is gezien de pogingen om via de EU de vingerafdrukverplichting voor ID-kaarten in te gaan voeren. En hopeloos vermoeiend voor de tegenstanders van biometrische ID-kaarten die (onder protest over de digi gezichtsopname en RFID opslag) in 2014 een vingerafdrukvrije ID-kaart hadden aangevraagd die nu weer bijna verlopen was. Waardoor bij nieuwe ID-kaart aanvragen er voor de betrokken aanvragers van een nieuw document, en voor de burgemeesters die in deze het bevoegd gezag uitoefenen, niks anders in het verschiet lag eind 2018 om opnieuw de hele bezwaar en beroepsprocedure weer over te doen, om niet het risico te lopen dat deze over de vorige aanvraag in de processtukken bij het EHRM als gedateerd niet meer geldig zouden zijn.



Varia aan privacy kwesties

Naast de hoofddossiers speelden door het jaar heen nog tal van onderwerpen, waar we bij betrokken waren. Zo noemen we in willekeurige volgorde:

De doorbraak in de kwestie BTW-BSN-ZZP weg ermee.

Eind in zicht van bulk verkoop klantgegevens door de Kamer van Koophandel.

Verbod van hogerhand op gemeentelijke verplichting tot elektronisch betalen.

Zaken die met het ongeoorloofd gebruik van het BSN te maken hebben.

Biometrische identificatie van werknemers en klanten.

Een varia aan zogenaamde 'slimme technologische ontwikkelingen' waarbij Vrijbit gevraagd werd om in kwesties variërend van initiatieven als smart-city, de promotie van oplaadpunten voor zelfrijdende auto's t/m op afstand uitleesbare thermostaten toelichting te geven over onderbelichtte aspecten als privacyrechten en samenhang tussen de voorgenomen energietransitie en de ontwikkeling van smart grid systemen.

Strijd tegen kentekenregistratie voor andere doeleinden dan verkeersovertredingen.

Verboden cameratoezicht door particulieren in de publieke ruimte.

Facebook terreur. Met name problemen met de moeilijkheid hoe het ongevraagd fotograferen en filmen van gezichten een halt toe te roepen. En steun aan initiatieven om mensen over te halen van Facebook 'af' te gaan.

Tegenwerking door bedrijven en overheidsinstellingen bij rechtmatige inzageverzoeken.

Waarbij met name de verwikkelingen naar aanleiding van de inzageverzoeken die Vrijbit bij de AIVD en MIVD indiende leidde tot ingewikkelde en omvangrijke bezwaar- en beroepsprocedures tegen de afwijzing op inzage wegens de beschuldiging van misbruik van macht. Actie tegen de vernietiging van een groot deel van de archieven van de AIVD en MIVD.

Digi-dwang en dwang, vanuit gemeentes, Belastingdienst, UWV e.a.

De aanvullende ID-plicht bij verkiezingen.

Tegenwicht bieden aan (al dan niet moedwillig) creëren/ in stand houden van valse mythes, nepnieuws, drogredenen en geschiedvervalsing.

Registratiedrift in onderwijs

Betaald parkeren volgens betaaldienst Dip&Go

Voorbereiden consequenties nieuwe betaaldienst PSD2

Intern functioneren

<u>Informatie-Documentatie</u>

Intern bestond het werk van de vereniging weer voor een belangrijk deel uit het verzamelen en verwerken van de gigantische hoeveelheid informatie op het gebied van privacybeperking die dag na dag beschikbaar kwam via publicaties, media, presentaties, symposia, debatten etc.

Dit verzamelen en verwerken van informatie is nodig om op de hoogte te blijven van actuele ontwikkelingen om ons informatie/advieswerk, hulpverlening, politieke lobby en juridische procedures te kunnen onderbouwen met relevante informatie.

Wekelijks werd zowel het digitale als het knipselarchief bijgewerkt.



Dagelijks publiceerde onze medewerker van de Privacynieuwsdienst artikelen met relevante actuele informatie. Waarvan ook wekelijks een nieuwsbrief gemaakt werd.

Privacynieuwsdienst 2018
803 artikelen geplaatst.
In 2018 trok de website privacynieuws.nl 1.289.804 bezoekers.
Die gezamenlijk 7.200.982 artikelen gelezen hebben.
Het aantal abonnees van de nieuwsbrief groeide van 841 naar 916

- Op individuele basis verzorgden we daarnaast via mail en 'life' gesprekken informatie over tal van privacyonderwerpen:
    - Via inbreng bij tal van debatten en bijeenkomsten over de Privacy.
    - Aan andere Burgerrechtenorganisaties
    - Aan de pers
    - Aan de regering, Tweede en Eerste Kamer, B&W's in Nederland en leden van gemeenteraden
    - Aan de Autoriteit Persoonsgegevens, het Rathenau instituut en de Kiesraad
    - Aan de rechtbank
    - Aan netwerkbeheerders, woningbouwverenigingen, en de Vereniging Eigen Huis.
    - Aan het UWV, de Belastingdienst en Kamer van Koophandel
    - Aan het Nederlands Juristen Comité voor de Mensenrechten(NJCM) het Public Interest Litigation Project (PILP), Platform Bescherming Burgerrechten, Bits of Freedom en Stichting Privacy First
    - Aan de vereniging van praktijkhoudende huisartsen, de stichting KDVP, de Stichting Beroepseer en actiecomité Stop Benchmark ROM
    - Aan de Stichting ondersteuning ongedocumenteerden STIL
    - Aan leerlingen en studenten in verband met studieprojecten.

Hulpverlening

De meeste vragen om hulp kwamen binnen via e-mail. Vaak rechtstreeks omdat mensen onze vereniging kenden of via internet ontdekten dat wij ons met bepaalde onderwerpen bezig houden. Regelmatig klopten mensen ook aan die door andere 'privacyorganisaties' waren doorverwezen. Ook kwam het regelmatig voor dat mensen die ons tegenkwamen en ter plekke hulp vroegen.

Die vragen betroffen een zeer uiteenlopend scala aan onderwerpen. We noemen in dit verband in willekeurige volgorde: de 'slimme meters', de algemene identificatieplicht, identificatieplicht banken, de vingerafdrukplicht voor paspoorten, eisen tot afgifte van biometrische persoonsgegevens door werkgevers en voor de justitiële DNA databank , ongewenst cameratoezicht en WIFI tracking in de publieke ruimte, screening door zorgverlenende instanties, plicht tot afgeven van persoonlijke gegevens voor het aanvragen sociale voorzieningen, kentekenparkeren, digi drang en dwang, problemen met ziekenhuis apotheken die weigerden om door de arts voorgeschreven medicijnen te verstrekken als mensen geen toestemming gaven voor het EPD-LSP.

De hulpverlening varieerde qua zwaarte. In een deel van de gevallen konden mensen veel zelf doen en vroegen voornamelijk om raad of om conceptbrieven na te kijken. Maar ook waren er mensen die niet zelf konden bedenken waar te beginnen om een probleem op te lossen. Hulpvragers voor wie wij telefoontjes moesten plegen omdat ze dat zelf niet konden, brieven of bezwaarschriften moesten opstellen en die van begin tot einde begeleiding nodig hadden om bepaalde problemen op te lossen.

Websites

Om onze doelstellingen te verwezenlijken onderhouden wij de volgende 7 websites:

- https:// www.vrijbit.nl
- https:// www.privacynieuws.nl

- https:// www.id-nee.nl
- https:// www.ikgeentoestemming.nl
- https:// www.wijvertrouwenslimmemetersniet.nl
- https:// www.louisetegendepaspoortwet.nl

Naast het technisch onderhoud en de beveiliging van de websites werd ook dit jaar weer verder geïnvesteerd in het publiceren van nieuwe artikelen en 'up to date ' houden van de diverse chronologische overzichten van verschillende dossiers. Met name het bijhouden van het 'CHRONO' over de jacht op onze medische gegevens vormde op zich al een flinke klus.

Vergaderingen

Iedere eerste zondag van de maand (met uitzondering van augustus) vond er een ledenvergadering plaats van 14-16 uur op onze locatie Kruisweg 32 in Utrecht. Belangstellenden waren op aanvraag welkom.

Tijdens deze bijeenkomsten kregen aanwezigen het verslag van de werkzaamheden van de afgelopen maand uitgereikt en de notulen van de vorige vergadering. Aan de orde kwamen verder:

- Toelichting op de stand van zaken van de actueel onder handen zijnde dossiers,
- Privacynieuws en overzicht van komende (privacy gerelateerde) bijeenkomsten, en
- De mogelijkheid om bepaalde onderwerpen uit te diepen en/of te brainstormen over aanpak en werkwijze van Vrijbit.

Daarnaast vond in juni de statutair verplichtte Algemene Leden Vergadering plaats. Waar het jaarverslag, de beleidsvoornemens, bestuurswisseling en vaststelling van de kascommissie aan de leden ter stemming werden voorgelegd.

Werkverslagen

Voor intern gebruik werd maandelijks een nauwgezet overzicht bijgehouden van alle activiteiten.

Slechts een klein deel van de leden was in de gelegenheid om zich actief in te zetten voor het Vrijbitwerk. De werkzaamheden bestonden daarbij vaak uit de inzet voor kwesties waar men persoonlijk via een aantasting van de privacy bij betrokken was geraakt. Sommige leden leverden een bijdrage op grond van hun specifieke kennis of vaardigheden op een specifiek gebied of met betrekking tot specifieke dossiers. Anderen hielpen met het verspreiden van actiemateriaal, bezoeken van bijeenkomsten, brainstormen over hoe zaken aan te pakken, ontwerpen van actiemateriaal, het organiseren van bijeenkomsten etc.

Ledenadministratie

Ook het bijwerken van de ledenadministratie gebeurde op maandelijkse basis. Het ledenaantal bleef door diverse lidmaatschappen die niet verlengd werden en nieuwe aanmeldingen die daarvoor in de plaats kwamen tussen de 200 en 225 leden schommelen.

In 2018 zijn opnieuw twee leden van Vrijbit overleden.

Jubileum





Op 24 juni 2018 bestond Burgerrechtenvereniging Vrijbit 10 jaar. Ondanks alle somber stemmende onderwerpen op gebied van de privacy vonden we dit voldoende gedenkwaardig om er een feestelijke en inspirerende middag van te maken voor en met onze leden en mensen waar we in de loop van die 10 jaar mee te maken hadden gehad.

Het werd inderdaad een bijzondere middag, met voordrachten, videoboodschappen, muziek, een tentoonstelling van de posters die de afgelopen 10 jaar het licht zagen in verband met privacybijeenkomsten en acties, een ludiek optreden van kardinaal Titus, de prijsuitreiking van de Privacyaward-2018, gedichten, educatieve spelletjes, een muzikaal sprookje, lekker eten en een symbolisch kampvuur.








1984
BIG BROTHER AWARDS


Freiheit statt Angst
DEMO
IN BERLIN
Samstag
11.09.2010
BIG BROTHER AWARDS
EDITIE 2011
7 MAART 2012
PRIVACY PLATFORM
A COMPREHENSIVE DATA PROTECTION FRAMEWORK
Cleveringadebat 2010
Privacy... gevoelig?

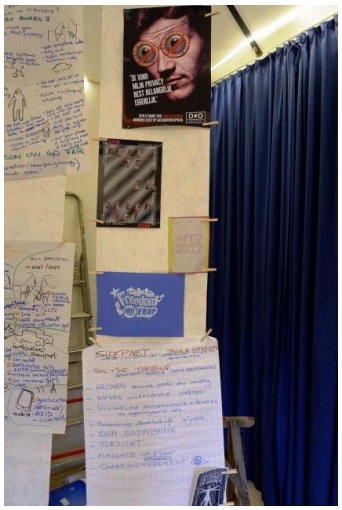

ID NEE
VRIJBIT
OBSERVATOR
HOW TO BE SEEN


PRIVACY PLATFORM
A COMPREHENSIVE DATA PROTECTION FRAMEWORK
Cleveringadebat 2010
Privacy... gevoelig?
dag van de privacy
PAS OP U WORDT GEVOLGD
BIG BROTHER OUDERWETS

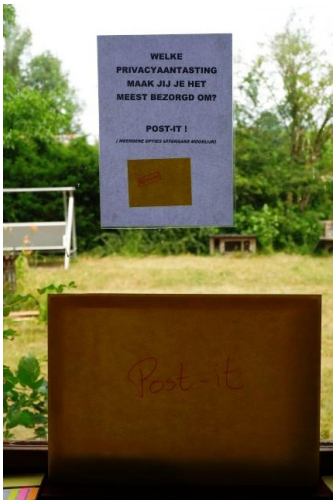

BIG BROTHER AWARDS
1984
Privacy Platform Meeting
PRIVACY PLATFORM
COUNTER CULTURE FESTIVAL
FREE ENTRANCE


Privacy... gevoelig?
BIG BROTHER OUDERWETS
CULTURE FESTIVAL
BIG BROTHER IN EUROPA


SLIM METEN = SLINKS WETEN
Freiheit statt Angst
DEMO
IN BERLIN
Samstag
11.09.2010
BIG BROTHER AWARDS
EDITIE 2011
7 MAART 2012
PRIVACY PLATFORM
A COMPREHENSIVE DATA PROTECTION FRAMEWORK







Financieel jaaroverzicht 2018

Saldo 1/1/2018 bedroeg € 7.557,22

Saldo 31/12/2018 was € 4.670,81

<u>BALANS 2018</u>

Saldo 1-1-2018	totaal	€ 7.557,20
Inkom 2018	totaal	€ 6.739,69
		---------- +
		€ 14.296,89
Uitgaven 2018	totaal	€ 9.626,08
		---------- -
Saldo 31-12-2018		€ 4.670,81

Inkomsten in 2018 bestonden voornamelijk uit de contributies á € 1.245,00 en donaties ten bedrage van € 4.892,42. Overige inkomsten werden gevormd door eenmalige restitutie van griffiekosten, opbrengt bijeenkomsten en verkoop actiemateriaal.

Uitgaven werden gevormd door de volgende posten:

Actiemateriaal € 428,43

Internet/telefoonkosten € 787,37

Webkosten € 1.775,56

Bureauartikelen € 211,43

Catering € 907,27

Frankeerkosten € 256,49

Literatuur € 82,99

Kranten € 979,50

Griffie € 676,00

Auteursrecht € 140,15

Reiskosten € 595,60

Betaalverkeer € 168,14

Verblijfskosten € 40,47

Advertentiekosten € 150,00

Huur locaties € 1.043,00

Entree en bijdrage bijeenkomsten € 608,75

Restitutie foutieve boeking € 655,35

Dat er ondanks de beperkte financiële middelen zoveel werk verzet werd is te danken aan de inzet van de vrijwilligers die zich, zonder enige onkostenvergoeding, inzetten zodat alle inkomsten voor 100% rechtstreeks aan het werk ten goede komen.

Via deze weg willen we, ook dit jaar weer, deze mensen hartelijk danken voor al hun tijd en energie. Ook alle donateurs danken we nogmaals voor hun onmisbare steun!

Namens het bestuur,

J.M.T.(Miek) Wijnberg, voorzitter