

Amsterdam, juli 2015

Visie op Privacy 2.0

Privacy vormt de basis van onze democratische rechtsstaat. Privacy is een mensenrecht en fundamentele vrijheid en omvat naast de persoonlijke levenssfeer en ontwikkeling ook de bescherming van persoonsgegevens, vertrouwelijke communicatie en integriteit van persoon en lichaam. Het universele recht op privacy is een vereiste voor het kunnen uitoefenen van andere vrijheden, zoals de vrijheid van meningsuiting en vrije pers. Het recht op privacy staat de laatste jaren echter onder grote druk. Privacy First vindt dat dit recht verdedigd moet worden door het te versterken en ziet privacy juist als een kans. Een kans voor bedrijven en organisaties om zich te profileren als privacyvriendelijk en een kans voor Nederland om internationaal een gidsland te zijn op het gebied van privacy.

Om van Nederland een gidsland op privacygebied te maken, zien we een aantal vergezichten en concrete handvatten. Met onze visie willen we een klimaat van voortdurend onderzoek en reflectie op privacyvraagstukken stimuleren. Gelukkig zijn wij niet de enigen in Nederland die zich sterk maken voor privacy. Steeds meer bedrijven en burgers zien in dat privacy geen belemmering voor innovatie vormt, maar juist een kans. Privacy First wil dit visiedocument dynamisch maken om mensen met goede ideeën de ruimte te bieden om bij te dragen aan een continue discussie over privacy in de Nederlandse samenleving. Bent u zo iemand met een goed idee? Of heeft uw organisatie ervaring op dit gebied die u graag wilt delen? We zoeken mensen die 'Part of the Solution' willen worden en met ons meedenken over een toekomstig privacyvriendelijk Nederland. [Doe mee!](#)

Privacy als uitgangspunt voor innovatie

In de visie van Privacy First geldt privacy als uitgangspunt van ontwikkeling en innovatie. Privacyvriendelijk opereren is de standaard en het is ondenkbaar dat bedrijven en overheden de privacy van mensen schenden. Concreet uit zich dat in de volgende punten:

Standaard Privacy by Design & Privacy Impact Assessments

'Privacy by design' wordt als uitgangspunt wettelijk vastgelegd. De [zeven fundamentele principes](#) van 'privacy by design' vormen het vertrekpunt bij de ontwikkeling van nieuwe technologie, diensten en producten. Een voorbeeld hiervan is dat 'privacy by default' standaard wordt toegepast. Projecten en wetsvoorstellen worden opengesteld voor publieke evaluatie. Voorstellen die gelijke functionaliteiten of effecten hebben, maar vriendelijker zijn voor privacy, krijgen de voorkeur boven minder privacyvriendelijke voorstellen. In aanbestedingsprocedures bij de overheid wordt privacyvriendelijkheid opgenomen als toetsingscriterium. Bij wetgeving en projecten van overheden en bedrijven die mogelijk invloed hebben op de privacy worden altijd onafhankelijke [privacy impact assessments](#) gedaan die openbaar beschikbaar zijn.

Het no-go/go principe bij grote projecten

Grote projecten bij de overheid en het bedrijfsleven werken volgens de no-go/go methode. Wanneer een fase van een project wordt opgeleverd zonder dat er afdoende privacybeschermende maatregelen zijn getroffen, mag het project niet verder. Zo wordt voorkomen dat systemen die op privacygebied nog niet op orde zijn, desondanks jarenlang proefdraaien en in gebrekkige staat in gebruik raken.

Systemen en processen worden ontworpen voor hun specifieke doel

Persoonsgegevens en data die betrekking hebben op personen mogen alleen worden verwerkt voor het vooraf bekende doel. Systemen en processen worden ingericht voor het doel waarvoor ze bestaan. Technieken die *function creep* (doelverschuiving) in de hand werken, zoals centrale dataopslag, omkeerbare pseudonimisering en vage of te ruime bevoegdheden zijn niet toegestaan. Dergelijke systemen en projecten worden derhalve negatief beoordeeld in de privacy impact assessment en kunnen niet worden gerealiseerd totdat doelbinding in het systeem is ingebouwd.

Burgers maken echte vrije keuzes

Momenteel is de positie van consumenten tegenover bedrijven zwak. Het is onmogelijk om te weten wat de voorwaarden zijn van alle diensten en producten die we gebruiken. Dit komt doordat voorwaarden te lang, moeilijk leesbaar en te weinig concreet zijn. “Vertrouw ons en teken bij het kruisje” is de boodschap. Derhalve weten burgers niet wat er met hun persoonsgegevens en gegenereerde data gebeurt. Dit leidt tot wantrouwen jegens bedrijven en tot maatschappelijk onbehagen, met name ten aanzien van innovatie. Technologie wordt daarom in de visie van Privacy First juist ingezet om de vrije keuze op het gebied van privacy van Nederlanders ten goede te komen. Burgers kunnen zelf weloverwogen vrije keuzes maken over hoe zij met hun persoonlijke data omgaan. Hiertoe worden de volgende zaken gerealiseerd:

De voorwaarden voor producten en diensten zijn begrijpelijk en toegankelijk

Privacyverklaringen en algemene voorwaarden zijn toegankelijk en duidelijk voor iedereen. Dat betekent dat ze maximaal één pagina tekst beslaan en in begrijpelijke taal zijn geformuleerd, vanuit het perspectief van de consument. Daarnaast worden gestandaardiseerde pictogrammen gebruikt die in één oogopslag de belangrijkste elementen van de voorwaarden samenvatten. Ook kunnen burgers gratis, snel en eenvoudig hun gegevens opvragen bij bedrijven waar zij klant zijn en bij de overheid, volgens gestandaardiseerde formulieren. Indien de gegevens onjuist zijn, kunnen deze eenvoudig worden gecorrigeerd en wordt deze correctie doorgetrokken in de gehele keten.

Iedereen in Nederland is goed geïnformeerd over verantwoorde omgang met persoonsgegevens

Overheden, bedrijfsleven en burgers nemen een gezamenlijke verantwoordelijkheid voor het in brede zin informeren van de Nederlandse bevolking en het bedrijfsleven over hoe zij zorgvuldig kunnen omgaan met persoonsgegevens. Dit betekent dat er in de samenleving in het algemeen en in het onderwijs in het bijzonder ruimte is voor bewustwording van risico's omtrent het delen van persoonsgegevens, zowel op het internet als offline. Het curriculum van het onderwijs draagt bij aan het opgroeien van alle kinderen tot digitaal-bewuste personen. Aangezien technologische ontwikkelingen ook veranderingen in gedrag kunnen vereisen, worden deze curricula regelmatig geactualiseerd en zijn deze toegankelijk voor de gehele bevolking.

Niemand is verplicht om gegevens af te staan die niet direct relevant zijn

Om een daadwerkelijke keuze te hebben over hun persoonsgegevens, worden burgers nooit uitgesloten van bepaalde diensten als zij weigeren om bepaalde gegevens af te staan die niet direct noodzakelijk zijn voor de betreffende dienst. Dit geldt met name voor het internet, bijvoorbeeld bij het niet accepteren van *tracking cookies*, het niet toestaan van locatiegegevens of niet geven van je geboortedatum. Tevens hebben burgers de mogelijkheid om standaard privacy-instellingen in te stellen naar hun eigen wensen en kunnen zij bijvoorbeeld een digitaal dashboard gebruiken om per dienst of website bepaalde voorkeuren af te stellen. Dit principe wordt ook meegenomen bij de toetsing van mogelijke kartelvorming en monopolies; er moet altijd een privacyvriendelijk alternatief bestaan voor consumenten.

Nederland als internationaal gidsland

In de visie van Privacy First wordt Nederland een privacy gidsland. Andere landen kijken naar ons, hoe we een veilige thuishaven zijn voor schrijvers, kunstenaars, klokkenluiders en vrije burgers. Ze kijken naar de verbinding tussen privacy en bedrijfsmatige innovatie en concurrentie. De verantwoorde omgang met persoonsgegevens door overheden en bedrijfsleven geeft impulsen aan innovatie. Bedrijven zien de Nederlandse omgang met privacy als een *unique selling point*, waarmee ze het vertrouwen van klanten winnen. Nederland is een land waarin mensen vrij zijn en zich vrij voelen om in het maatschappelijk verkeer te bewegen. Concreet betekent dat dat de volgende punten het Nederlands beleid kenmerken:

Persoonsgegevens zijn geen handelswaar

Privacy vormt een mensenrecht en een basis voor andere fundamentele vrijheden waar Nederland zich traditiegetrouw sterk voor maakt. Persoonsgegevens en andere data hebben echter ook een economische waarde. Te vaak worden de fundamentele vrijheden ingeruild voor economische belangen, vaak zelfs zonder dat de persoon op wie de data betrekking hebben hiervan op de hoogte is. In Nederland is privacy geen onderdeel van de *package deal*. Nederlandse overheden mogen persoonlijke gegevens niet onderling noch internationaal uitwisselen zonder directe aanleiding en wettelijke waarborgen. In internationale onderhandelingen zet Nederland zich in voor een aparte status van privacy binnen verdragen en beleid, opdat de internationale kapitalisatie van persoonsgegevens wordt beëindigd.

Nederland zet zich in tegen massasurveillance

In Nederland vindt geen massasurveillance plaats. Het aftappen van telefoongesprekken, lezen van e-mails en berichten en hacken van computers is alleen toegestaan wanneer iemand met rede verdacht wordt van een concreet strafbaar feit en slechts na voorafgaande rechterlijke toetsing. Hierbij geldt een zeer strenge interpretatie van de principes van noodzakelijkheid en proportionaliteit. De biometrische gegevens van alle burgers worden nimmer opgeslagen in centrale databanken. Nederland maakt zich sterk voor beëindiging van massasurveillance in andere landen en accepteert geen massasurveillance van Nederlanders door andere landen. Plannen waarbij de overheid stelt dat privacy is gewaarborgd worden door onafhankelijke partijen getoetst.

Nederland neemt strategische hard- & software posities in

Bepaalde strategische internet- en privacyposities worden in Nederland bewaard en gestimuleerd, zoals cryptografische software en algoritmes. Persoonsgegevens van en data die betrekking hebben op Nederlanders worden opgeslagen op Nederlandse servers en in de Nederlandse [cloud](#), zodat de

Nederlandse wetgeving van toepassing is. Tevens is accurate beveiliging van de data gegarandeerd en zijn bedrijven verantwoordelijk voor de beveiliging van de persoonsgegevens van hun klanten.

Bedrijven en overheden nemen hun verantwoordelijkheid

In de visie van Privacy First hebben geïnformeerde burgers de controle over hun persoonsgegevens terug en houden zij bedrijven en overheden aansprakelijk voor de zorgvuldige omgang met deze gegevens. Transparantie, controle en aansprakelijkheid zijn hierbij sleutelwoorden. Deze uiten zich in de volgende punten:

De gehele keten is verantwoordelijk voor zorgvuldig databeheer en aansprakelijk als het misgaat

Verantwoorde omgang met persoonsgegevens en andere data is een verantwoordelijkheid van alle bedrijven van een keten, vergelijkbaar met de [ketenverantwoordelijkheid](#) bij maatschappelijk verantwoord ondernemen. Ook zorgen alle bedrijven in de keten er gezamenlijk voor dat datalekken worden voorkomen en adequaat gedicht. Datalekken worden ook direct gemeld bij het centrale meldpunt en eventueel getroffen personen worden hierover geïnformeerd en ontvangen compensatie.

Toezichtsorganen en het parlement handhaven en controleren omgang met persoonsgegevens

Er is stevige parlementaire controle op omgang met persoonsgegevens door alle overheidsinstanties. Ook heeft de Autoriteit Persoonsgegevens (het huidige College Bescherming Persoonsgegevens) een grote rol, ruime bevoegdheden en de mogelijkheid om serieuze sancties op te leggen bij onzorgvuldige omgang met persoonsgegevens. De sancties zijn van dien aard dat het nooit aantrekkelijk is voor een bedrijf om de regels omtrent bescherming van persoonsgegevens te overtreden. Het CBP controleert ook overheidsorganen, politie, justitie en inlichtingen- en veiligheidsdiensten. Andere instanties zoals de Nationale Ombudsman en de Autoriteit Consument & Markt hebben ook een verantwoordelijkheid om de privacy van individuen te beschermen en misstanden aan te pakken. Tevens is constitutionele toetsing door de rechter grondwettelijk verankerd zodat privacyschennende wetgeving door de rechter ongrondwettelijk kan worden verklaard.

Visionaire denkers en ideeën gezocht

Privacy First organiseert bijeenkomsten waarin we nadenken over een toekomstig privacyvriendelijk Nederland. Dit kan bijvoorbeeld gaan over privacyvriendelijke 'slimme meters', icoontjes om de privacyverklaringen van websites te verbeteren, of het veiliger waarborgen van onze gevoelige gegevens in [Suwinet](#), het informatie uitwisselingssysteem van de overheid. Dit kunnen wij echter niet alleen. We zijn ervan overtuigd dat er heel veel mensen in Nederland goede, visionaire ideeën hebben over privacy! Heeft u ideeën om Nederland privacy gidsland te maken? Of om bedrijven privacyvriendelijker in te richten waarbij tegelijkertijd de veiligheid van de systemen wordt versterkt? [Denk dan met ons mee!](#)