4 Privacy en profielensites

Privacy houdt niet op bij de voordeur. Ook in het openbare leven, en dus ook bij wat je doet op internet, heb je recht op bescherming van je privacy, in mooi juridisch je 'persoonlijke levenssfeer.'[1] Gebruik van privé-gegevens is aan strenge regels gebonden. Mag je werkgever bijhouden welke sites je bezoekt onder werktijd? Zijn die maandelijkse reclamemails van die webwinkel waar je ooit wat gekocht had eigenlijk wel legaal? En wat mag iemand doen met de informatie op je Hyves-profiel?

Wet op de privacy

Er bestaat in Nederland geen algemene "wet op de privacy". Er zijn diverse wetten die elk een bepaald aspect van de privacy in Nederland regelen. De belangrijkste en bekendste wet is de Wet Bescherming Persoonsgegevens. Deze regelt hoe persoonlijke gegevens mogen worden opgeslagen en verwerkt. Regels over aftappen en afluisteren staan weer in de Wet Computercriminaliteit en in de Telecommunicatiewet. Het briefgeheim is vastgelegd in de Grondwet (maar geldt dan weer niet voor e-mail).

De **Wet Bescherming Persoonsgegevens** (WBP) regelt onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn alle gegevens die **herleidbaar zijn tot een bepaald individu**.[2] Het bekendste voorbeeld is iemands naam of adres. Maar aan een foto is iemand ook te herkennen. Een foto is dus net zo goed een persoonsgegeven.[3]

En het houdt niet op bij zulke feitelijke gegevens: gegevens die een waardering over een bepaalde persoon inhouden, bijvoorbeeld iemands IQ, kunnen ook persoonsgegevens zijn, als te achterhalen is welke persoon dit IQ heeft.

Omdat bijvoorbeeld een e-mailadres of MSN-account ook een persoonsgegeven is, heeft deze wet ook de nodige consequenties voor internetaanbieders en -gebruikers. Het publiceren van persoonsgegevens van anderen op internet valt namelijk al snel onder de strenge regels van de WBP.[4]

Gebruiken van persoonsgegevens mag alleen met toestemming of wanneer het past binnen het doel waarvoor je ze hebt verkregen.

Toestemming nodig

Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de regels van de WBP. Uitgangspunt is dat de betreffende persoon zijn **toestemming moet hebben gegeven** voor de verwerking.[5] Worden gegevens gevraagd aan die persoon zelf, dan moet deze vooraf geïnformeerd worden over opname in het bestand. Zonder toestemming moet je een aantoonbare, zwaarwegende noodzaak hebben om die persoonsgegevens te gebruiken.

Een registratieformulier moet expliciet een aanvinkvakje hebben waarin de vereiste toestemming wordt gevraagd. De toestemming verstoppen in het reglement is niet genoeg.[6] (En helemaal niet als men zinnen gebruikt als "*Wij verbeteren uw gebruikservaring door geselecteerde informatie te delen met onze gewaardeerde partners*".) Bij persoonsgegevens die uit andere bronnen worden verzameld, moet de betreffende persoon worden geïnformeerd bij het moment van opname of uiterlijk net voor het moment van verstrekking aan derden.[7]

Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de legitieme doeleinden waarvoor ze zijn verkregen.[8] Het abonneebestand voor een internetnieuwsbrief mag je gebruiken om die nieuwsbrief rond te sturen, maar niet om de abonnees zomaar reclame te sturen.[9] Ook mag er niet meer worden verzameld dan noodzakelijk voor de afgesproken doelen.[10]

Bestanden met persoonsgegevens moet je **aanmelden bij het College Bescherming Persoonsgegevens**. Voor eenvoudige verwerkingen zijn er vrijstellingen.[11] Zo hoef je abonneebestanden voor nieuwsbrieven en de logfiles of statistieken voor je website niet aan te melden, mits je je maar houdt aan de regels van de betreffende vrijstelling.

Informeren, inzage en correctie

Alle organisaties die persoonsgegevens gebruiken, hebben een **informatieplicht**.[12] Dit betekent dat zij de personen op wie de gegevens betrekking hebben, moeten laten weten wat zij met hun gegevens gaan doen. Dit hoeft niet wanneer het vanzelfsprekend is (bijvoorbeeld bij het invullen van een

Wat mag er met IP-adressen van de privacywet?

Elke computer op internet krijgt automatisch een IP-adres toegewezen. Alleen de provider kan de link leggen naar de persoon achter dat IP-adres. Zulke IP-adressen zijn persoonsgegevens, omdat ze (via die provider) te herleiden zijn tot een natuurlijk persoon.[13] Dat geldt zelfs als je een rechtszaak nodig zou hebben om de provider tot afgifte te dwingen.[14] Het gevolg is dat een site niet zomaar IP-adressen van bezoekers mag publiceren. Bijhouden mag wel, bijvoorbeeld om misbruik of vandalisme tegen te kunnen gaan.

registratie-formulier bij een online forum) of wanneer het zeer tijdrovend is om het adres van de betrokkene te achterhalen.

Wie persoonsgegevens verwerkt, moet uitleggen welke **beveiligingsmaatregelen** hij heeft genomen om misbruik van persoonsgegevens te voorkomen.[15] Zo mag een databank met persoonsgegevens niet zomaar via internet toegankelijk zijn. De beveiliging moet afdoende zijn gezien het soort gegevens en de te verwachten bedreigingen. Bij een klantenbestand van een webshop gelden dus (iets) lichtere eisen dan bij een elektronisch patiëntendossier.

Daarnaast hebben personen die in een bestand zijn opgenomen het recht om hun geregistreerde gegevens in te zien. Dit geldt niet alleen voor tekstuele data, maar ook voor bijvoorbeeld audio-opnames en videobeelden.[16] Ook kunnen zij eisen dat hun gegevens **verbeterd, aangevuld, verwijderd of afgeschermd** worden.[17] Dat mag wanneer de gegevens die gebruikt worden feitelijk onjuist, onvolledig of niet ter zake dienend zijn voor het doel of de doeleinden van de verwerking. Een wanbetaler kan bijvoorbeeld niet verwijdering van

Mag mijn stamboom op internet?

Een familiestamboom bevat persoonsgegevens van iedereen die erin staat (naam, geboorte- en overlijdensdatum). Wil je deze op internet publiceren, dan moet je toestemming hebben van alle levende personen in de stamboom.[18] Houd er wel rekening mee dat bijvoorbeeld de partner of kinderen van een overledene gemakkelijk te achterhalen zijn wanneer er voldoende informatie over de overledene zelf wordt gepubliceerd. Die partner of kinderen moeten dan toestemming geven voor vermelding van de overledene.

zijn persoonsgegevens eisen bij de debiteurenadministratie van een bedrijf. Hij kan wel zijn nieuwe adres laten opnemen in die administratie. De beheerder van het bestand mag een verzoek alléén weigeren als het disproportioneel grote lasten op zou leveren.[19]

Privacyverklaring

Elke site moet een **privacyverklaring** hebben als ze persoonsgegevens verzamelt — al is het maar door een logfile bij te houden van de bezoekjes.[20] Daarin moet de site uitleggen welke gegevens worden verzameld van bezoekers en wat daarmee gebeurt. Dat hoeft niet met hele breedsprakige juridische formuleringen. Sterker nog, het is juist de bedoeling dat je in gewone taal uitlegt dat je logfiles bijhoudt en wat je daarmee doet.

Een site moet uitleggen welke gegevens ze over mensen verzamelt, wat ze daarmee doet en hoe dit beveiligd wordt. De betrokkenen hebben recht op inzage en correctie.

Veel mensen denken dat als een site een privacyverklaring heeft, het wel goed zit met hun privacy. Maar dat is niet altijd waar. Een privacyverklaring zegt alleen wat een bedrijf doet met persoonlijke gegevens van anderen. Doorverkopen aan adverteerders is toegestaan, als dat in de privacyverklaring staat.

Welke dingen horen er in een privacyverklaring aan de orde te komen? Een paar voorbeelden:

- **Webbezoek:** welke gegevens houdt de site bij over het 'klikgedrag' van bezoekers? En wat doet men daarmee? Wekelijkse statistieken maken, of doorverkopen aan adverteerders?

- **Cookies:** welke informatie wordt er via cookies bijgehouden?[21] Een cookie is een stukje informatie dat een server meestuurt met elke webpagina. De webbrowser stuurt het cookie mee terug, zodat de server bijvoorbeeld kan bijhouden welke pagina's een specifieke bezoeker allemaal leest. Daarmee kan een profiel van die gebruiker worden opgebouwd.

- **Zoekopdrachten:** bewaart de site zoekopdrachten om bijvoorbeeld te kunnen kijken wat populaire zoektermen zijn? Dat mag. Maar als de site ook bijhoudt welke bezoekers welke zoekopdrachten uitvoeren, dan moet men dat melden in de privacyverklaring.

- **Contactformulieren en -adressen:** wat gaat men doen met de gegevens die iemand invult in het contactformulier? Stuurt het bedrijf alleen een antwoordmail, of komt het adres meteen op de lijst voor direct mailings? En wat gebeurt er eigenlijk na het beantwoorden van zo'n mail met contactgegevens?

- **Nieuwsbrieven en andere mailings:** hoe wordt dit bestand samengesteld? Hoe komt iemand op een verzendlijst, en — belangrijker — hoe komt hij er weer vanaf?

- **Registratie van gebruikers:** als gebruikers van een site zich kunnen registreren, welke gegevens wil men dan weten en wat gebeurt daarmee? Zijn namen van mensen zichtbaar bij reacties die men achterlaat, of is er ergens een lijst met contactinformatie van geregistreerde gebruikers zichtbaar? Hoe kan een gebruiker zijn account weer opheffen? En worden zijn gegevens dan ook écht verwijderd?

Op de zwarte lijst

Omdat internet helaas vol zit met structureel irritante mensen, verspreiders van spam, vandalen en andere overlastplegers, gebruiken veel mensen filters en zwarte lijsten om ongewenste uitingen te blokkeren. Voor privépersonen is dat niet zo'n probleem, maar als een site mensen gaat blokkeren (en zeker als ze de zwarte lijst delen met anderen) dan kan zij tegen de privacywetgeving aanlopen. **Ook een zwarte lijst is namelijk een "verwerking" van persoonsgegevens.** De zwarte lijst moet dan "noodzakelijk voor een gerechtvaardigd belang" van de zwartelijsthouder zijn, en dat belang moet zwaarder wegen dan het privacybelang van de personen die op die lijst komen.[22]

Een winkel of website moet op een of andere manier kenbaar maken dat men een zwarte lijst beheert en hoe je daar op komt.[23] Ook moeten mensen in staat zijn om na te gaan dat zij op deze lijst staan, en hebben zij het recht om eraf gehaald te worden als blijkt dat hun vermelding onterecht was. Het College Bescherming Persoonsgegevens heeft hiervoor een checklist gepubliceerd.[24] Je kunt met andere woorden niet zomaar iemands IP-adres nemen en dat op een lijst zetten die je dan als grote verrassing publiceert als een lijst van "roze randdebielen".[25]

"Het moest van Google"

De privacyverklaring was al een hele tijd verplicht, maar pas in maart 2008 nam het aantal sites met expliciete privacyverklaring ineens flink toe. De reden? Google stelde het vanaf dat moment als eis voor sites die mee wilden doen aan Google AdSense, haar lucratieve dienst om advertenties op je site te kunnen tonen.[26] Zonder privacyverklaring geen uitbetaling door Google.

Briefgeheim op e-mail

De Grondwet garandeert dat 'telefoongesprekken, papieren post en telegraafberichten' geheim zijn. Dit briefgeheim geldt echter niet voor elektronische communicatie. Een voorgestelde grondwetswijziging eind jaren negentig om dit te veranderen, sneuvelde.[27] Dat wil echter niet zeggen dat e-mail nu vogelvrij is.

Wanneer iemand zich met een geraden wachtwoord of andere truc toegang verschaft tot andermans mailbox, pleegt hij een misdrijf: computervredebreuk (zie hoofdstuk 14).[28]

E-mail valt niet onder het briefgeheim. Een beheerder of provider die e-mail van klanten leest, is vaak wel strafbaar. En de ontvanger moet rekening houden met het auteursrecht.

Medewerkers van bedrijven die een telecommunicatiedienst aanbieden, zijn **strafbaar als ze kennisnemen van de inhoud** van die overgebrachte communicatie.[29] Dit geldt bijvoorbeeld voor mensen die bij een internetprovider werken, maar ook voor beheerders van webmaildiensten of discussieforums en netwerksites. Zij mogen e-mail of privéberichten van gebruikers dus niet zomaar lezen.[30]

De eerlijke ontvanger van een e-mail heeft met dit alles niets te maken. De mail was voor hem bestemd, hij zit in zijn mailbox, en het briefgeheim bestaat niet voor e-mail. Toch mag hij niet zomaar doen met die mail wat hij wil. Hij mag de inhoud delen met anderen — maar dat moet hij dan wel in zijn eigen woorden doen. Want op de tekst van de e-mail zelf zit meestal auteursrecht (zie hoofdstuk 6).

De ontvanger heeft een beperkt gebruiksrecht (licentie): hij mag de e-mail bewaren en printen, maar niet veel meer dan dat. Hij mag het **niet publiceren, ook niet in de vorm van een citaat.**[31] Zou de mail naar een mailinglijst zijn gestuurd, dan mag herpublicatie iets eerder – zelfs als er zo'n disclaimer onder staat die zegt dat de mail vertrouwelijk is.

Omdat er bij e-mail zelden een expliciete licentie zal zitten, is het de vraag of de verzender impliciet toestond dat het werk mocht worden gepubliceerd. Staat er bij dat de mail vertrouwelijk is, dan mag het natuurlijk niet. Stuurde hij de mail naar een mailinglijst, dan mag deze best in het archief van de lijst worden opgenomen. Stuurde hij de mail naar een mailinglijst met zo'n disclaimer dat het vertrouwelijk is, dan is dat dom van hem. Ook zo'n mail mag worden gearchiveerd.

Privacy en internetten op het werk

Privacy bestaat ook op de werkplek. Als werknemer mag je een 'redelijk niveau' van privacy verwachten op je werkplek.[32] Niet zo veel als thuis, maar ook niet totaal geen privacy.

Wanneer mag het beheer pb's lezen?

De meeste forumsoftware heeft de mogelijkheid ingebouwd om deelnemers elkaar privéberichten (pb's) te laten sturen. Alleen de ontvanger kan die dan lezen — en de beheerder natuurlijk, want de beheerder kan alles. Hij mag dat echter niet, tenzij hij een dringende reden heeft die te maken heeft met de goede werking van het forum. Een dringende reden kan bijvoorbeeld zijn dat iemands inbox verstopt is, dat de beheerder een bevel van justitie kreeg om de inhoud van een pb af te geven of dat de virusscanner aangaf dat er een probleem was met een bericht.

Dat geldt ook voor internetgebruik. De privacy van de werknemer gaat onder normale omstandigheden boven het bedrijfsbelang bij monitoren of loggen van internetgebruik. Pas bij een redelijk vermoeden van wangedrag mag de werkgever gaan observeren.[33]

De grenzen tussen privé en zakelijk vervagen namelijk steeds meer. Werkgevers moeten accepteren dat werknemers privézaken regelen en hun persoonlijke netwerk onderhouden onder werktijd. Net zo goed als werknemers moeten accepteren dat het werk niet altijd om vijf uur klaar is. Dit betekent dat een werkgever **niet zomaar privé-gebruik van internet volledig kan verbieden**. Dit geldt niet alleen voor het bezoeken van websites — "internetten op het werk" is een breed begrip. Denk bijvoorbeeld aan het lezen en versturen van e-mail, het lezen van berichten op forums, blogs en discussiesites, het downloaden en uitwisselen van bestanden (filesharing) en nog veel meer. Ook het onder werktijd voeren van privé-telefoongesprekken, al of niet met een bedrijfstelefoon, valt hieronder.

Privégebruik van internet op het werk kan niet zomaar worden verboden. Monitoren mag, maar in principe anoniem, tenzij er een concreet vermoeden van wangedrag richting een medewerker is.

Het moet natuurlijk wel gaan om **gebruik waarbij je een zekere privacy mag verwachten**. Bij het versturen van een e-mail is dat duidelijk het geval. Maar wie een bericht plaatst op een openbaar toegankelijk discussieforum, dat via Google te vinden is, moet niet gek opkijken als zijn werkgever daarmee aan komt zetten. Het is geen schending van je privacy als je werkgever dat bericht vindt en je er op aanspreekt.

Persoonsgegevens 2.0

Wie een weblog, forum of profiel op Hyves heeft, publiceert daarop persoonsgegevens over zichzelf — of over anderen. Die gegevens kunnen jarenlang online blijven staan, dankzij zoekmachines en andere sites die alles kopiëren en herpubliceren. Veel mensen staan daar niet bij stil.[33] Bovendien worden veel van deze "Web 2.0" diensten gratis aangeboden, maar wel volgestopt met advertenties. De beheerders bouwen vaak gedetailleerde interesseprofielen van hun deelnemers op.[34] Het gemak waarmee mensen dit alles tolereren, vond stichting Bits of Freedom dusdanig schrikbarend dat ze de *Big Brother Award 2007* uitreikte aan 'U', de actieve internetter.[35]

Om duidelijkheid te scheppen over wat er nu wel en niet mag met persoonsgegevens op internet, heeft het College Bescherming Persoonsgegevens (CBP) de *Richtsnoeren publicatie van persoonsgegevens op internet*[36] opgesteld. Deze Richtsnoeren leggen uit hoe het CBP vindt dat de regels over persoonsgegevens moeten gelden bij publicaties op internet. Het CBP stelt

Zijn mijn Twitterberichten privé?

Via microblogdienst Twitter kun je berichtjes van 140 tekens sturen over wat je op dat moment aan het doen bent. Die berichtjes zijn in principe voor iedereen te lezen. In een dergelijke situatie mag je juridisch gezien weinig privacybescherming verwachten. Wat je twittert, is voor de hele wereld te lezen en mag dan ook door de hele wereld gelezen en doorgestuurd worden. Ook als je er '@' voor zet om aan te geven dat je bericht voor één persoon bedoeld is. De enige uitzondering is als je gebruikmaakt van het "slotje". Een lezer moet dan weten dat het bericht privé is. Hij mag dan die berichten niet zomaar publiceren of doorgeven aan anderen.

zich daarbij wel héél streng op. De hoofdregel is dat een site **voor élk gebruik van persoonsgegevens toestemming** moet hebben van de persoon over wie het gaat. Dit kan een site bijvoorbeeld in haar privacyverklaring of gebruiksreglement vastleggen.

Strikt naleven van die strenge regels zal voor veel Web 2.0-diensten erg problematisch worden. Waar de nieuwe regels namelijk kort gezegd op neerkomen, is dat een deelnemer absolute zeggenschap krijgt over zijn bijdrage, ongeacht wat er later mee gebeurt. Zo mag je bijvoorbeeld gegevens herpubliceren die iemand zelf online zet, maar als die persoon ze weghaalt bij de bron, moet jij ze ook verwijderen.[37]

De beheerder van de site is verder aansprakelijk voor elk hergebruik dat niet de bedoeling was. Hij moet dus maatregelen nemen om dit te voorkomen. Oftewel: geen zoekmachines toelaten op de site.[38] De beheerder kan zelfs worden verplicht om berichten uit de cache-archieven van die zoekmachines te verwijderen.[39]

Hoe oud moet je zijn voor een Hyve?

Minstens zestien, tenzij je ouders het goedvinden. Bij sites als Hyves, Sugababes of Habbo Hotel worden persoonsgegevens van deelnemers gepubliceerd. Dat mag alleen met toestemming, en de wet zegt expliciet dat die toestemming door de ouders gegeven moet worden als de deelnemer nog geen zestien jaar is.[40] Als de toestemming niet gegevens is, kunnen ouders op elk moment het profiel laten verwijderen. Overigens moet deze toestemming gezamenlijk worden gegeven. Dat speelt vooral een rol bij gescheiden ouders.[41]

Dat wringt natuurlijk wel een beetje. Als het de zoekmachines zijn die persoonsgegevens herpubliceren op onverantwoorde wijze, moeten het dan niet juist de zoekmachines zijn die veel terughoudender moeten zijn met het indexeren, koppelen en tonen van persoonlijke informatie?[42]

Regels voor zoekmachines

In april 2008 kwam het Europese samenwerkingsverband van privacytoezichthouders (de 'Artikel 29-werkgroep') met een advies over privacy bij zoekmachines.[43] Daarbij ging het vooral om de privacy van *gebruikers* van zoekmachines. Veel zoekmachines houden namelijk tot in detail bij wie welke zoekopdrachten invoert, en op welke resultaten wordt geklikt. De zoekmachines gebruiken deze gegevens om de meest passende advertenties te kunnen tonen, en om de zoekresultaten te kunnen verbeteren.

Een site die persoonsgegevens van gebruikers publiceert, moet volgens het College Bescherming Persoonsgegevens voorkomen dat zoekmachines daar toegang toe krijgen.

De regels uit het advies zijn niet verrassend: zoekmachines moeten blokkades zoals robots.txt[44] respecteren, duidelijk aangeven welke informatie men verzamelt en deze zo snel mogelijk, maar uiterlijk na zes maanden weer weggooien (waar Google het niet mee eens is). Of anonimiseren, maar dat is een vrijwel onmogelijke opgave. En wie dat wil, kan zoekmachines aanschrijven met een verzoek tot inzage in het over hem opgebouwde profiel.

In oktober 2009 sommeerde de werkgroep van EU-privacytoezichthouders Google en andere zoekmachines op grond van dit

advies om haar bewaartermijn van persoonsgegevens van negen naar zes maanden terug te brengen.[45] Die blafbrief had weinig effect, waarop de werkgroep in mei 2010 een klacht bij de Amerikaanse *Federal Trade Commission* neerlegde in de hoop dat die dan zou gaan bijten.[46]

Hoe bewaak je je privacy op internet?

1. Besef goed wat je doet als je iets over jezelf publiceert op een forum of blog. Alles wat je schrijft, zal voor eeuwig op internet staan. In theorie kun je met de privacywet daar wat aan doen, maar de praktijk is anders.
2. Wees terughoudend met het invullen van naam- en adresgegevens op websites. In veel gevallen heeft een site je adres en telefoonnummer nergens voor nodig.
3. Lees de privacyverklaring van een site voordat je je registreert. Als dan nog onduidelijk is wat een site gaat doen met je gegevens, vraag het ze dan eerst.
4. Gebruik een tijdelijk e-mailadres om je te registreren bij websites, en gebruik je 'echte' e-mailadres alleen voor privécorrespondentie.
5. Let op wat voor cookies een site allemaal meestuurt. In de meeste browsers is het accepteren van cookies uit te zetten, of kan per cookie toestemming worden gegeven of geweigerd.
6. Ga er vanuit dat alles wat je op je Hyves-profiel, Linkedinpagina, blog of homepage zet, voor de hele wereld toegankelijk is. Ook als je de site afschermt voor een beperkt groepje vrienden. Je weet immers nooit wat een van je vrienden met die informatie zal doen.
7. Als je iets publiceert over anderen, bijvoorbeeld een groepsfoto of een blogbericht, vraag je dan altijd af of die anderen het wel zo leuk vinden om met naam en gezicht op internet te komen.