HET RECHT OP INZAGE IS EEN WASSEN NEUS. WAT NU?

Jaap-Henk Hoepman, Senior Scientist, TNO & Radboud Universiteit Nijmegen

Volgens de Wet bescherming persoonsgegevens (Wbp) heeft iedere burger het recht om inzage te krijgen in de persoonsgegevens die een organisatie over haar verwerkt. Tevens moet deze organisatie informatie geven over het doel van de verwerking, de herkomst van de persoonsgegevens, en een overzicht van organisaties waaraan deze gegevens eventueel zijn verstrekt. Recent heeft Bits of Freedom een tool gelanceerd waarmee burgers zo'n inzageverzoek eenvoudig kunnen genereren: de Privacy Inzage Machine (PIM)[1]

In het kader van het Privacy Seminar dat ik ieder voorjaar geef aan de Radboud Universiteit Nijmegen, heb ik mijn studenten begin 2011 gevraagd om bij een aantal organisaties gebruik te maken van dit recht. We hebben hiervoor een beta-versie van PIM gebruikt. Zelf heb ik dat ook gedaan.
Doel was om te kijken hoe organisaties met dergelijke inzageverzoeken omgaan. De conclusie is ontluisterend: dat doen ze beroerd. Het recht op inzage is in de praktijk een wassen neus.

> Reageren op inzageverzoeken: de conclusie is ontluisterend, dat doen ze beroerd

We hebben de klantenservice van telecommunicatiebedrijven, verzekeringsmaatschappijen, webwinkels, supermarkten en dergelijke aangeschreven. De meerderheid (70% in deze beperkte steekproef) van de bedrijven en organisaties reageert simpelweg niet. Van de bedrijven en organisaties die wel reageren, kunnen we stellen dat de reactie zelden voldoet. Sommige bedrijven sturen geen brief maar bellen. Andere bedrijven sturen een e-mail, of een korte brief die niet ingaat op het verzoek maar enkel meedeelt: "Verder worden uw persoonsgegevens nooit vrijgegeven aan andere organisaties. U hoeft zich dus hierover geen zorgen te maken." We ontvingen ook een uitdraai van iets wat lijkt op een screenshot van een persooneelsadministratiesysteem. Daar staan wij niet in, inderdaad... De klantenservice van een ander bedrijf belt een student met de vraag of hij echt een inzageverzoek wil doen. De medewerker is al uren bezig met dit verzoek en nog steeds niet klaar.

De enige twee organisaties die het goed doen zijn de Gemeentelijke Basis Administratie (GBA) en Bol.com. Het antwoord van de GBA komt laat (na drie weken), maar bevat een uittreksel van alle gegevens die de GBA over de persoon in kwestie opgeslagen heeft, plus een overzicht van de gegevens die aan andere partijen zijn doorgegeven. Ook Bol.com reageert snel met een keurige brief met daarin alle gevraagde gegevens.

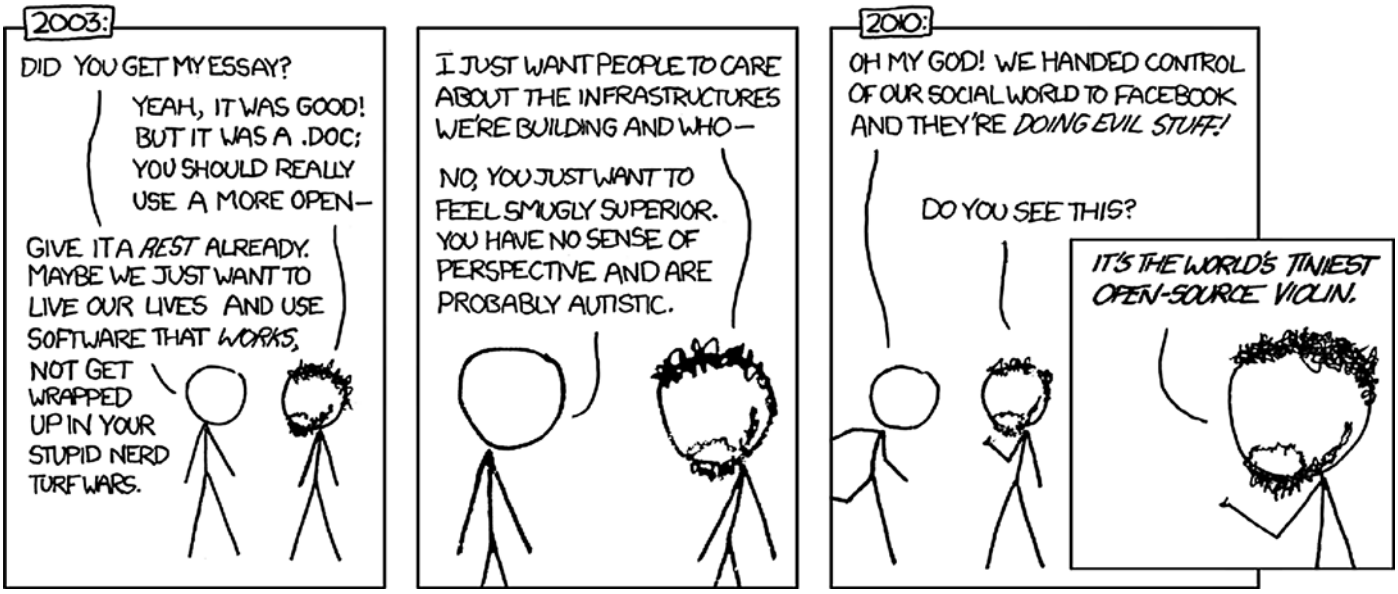
> Kennelijk zijn er geen goede bedrijfsprocessen geïmplementeerd

Al met al een teleurstellend resultaat. Bedrijven zijn wettelijk verplicht binnen een redelijke termijn een verzoek tot inzage volledig te beantwoorden.
Waarom reageren ze dan zo onbeholpen? Dat kan liggen aan het feit dat bedrijven over het algemeen maar weinig inzageverzoeken ontvangen. Zo is bekend dat ook maar weinig mensen Google Dashboard raadplegen (om te kijken hoe Google omgaat met de persoonsgegevens die ze bewaart). En omdat ze maar weinig verzoeken tot inzage krijgen, hebben ze kennelijk geen goede bedrijfsprocessen geïmplementeerd om zo'n verzoek correct te beantwoorden.

Dat laatste is wel opmerkelijk, en eigenlijk ook wel zorgelijk, en onzorgvuldig. De PIM-tool van Bits of Freedom bevat alleen bedrijven die officieel hebben gemeld dat ze persoonsgegevens verwerken. Ook dit is een verplichting die voortvloeit uit de Wbp. Kennelijk melden bedrijven netjes de verwerking van persoonsgegevens, maar laten ze vervolgens na de noodzakelijke processen voor het verwerken van een inzageverzoek goed in te richten. Dan rijst toch de vraag of deze bedrijven überhaupt hebben nagedacht over de verwerking van persoonsgegevens. Weten ze wel precies welke persoonsgegevens ze allemaal verzamelen, en hoe en waar dat precies gebeurt?
Dit vergroot de kans op incidenten en privacyinbreuken van de klant. Immers, als je niet weet welke informatie je verzamelt, en waar je die opslaat, verwerkt en gebruikt, dan kun je die informatie ook niet afdoende beschermen.

Hoe deze situatie te veranderen?
Bedrijven zouden kunnen overgaan tot

[1] [https://pim.bof.nl/]



Randall Munroe - xkdc.com/743 (CC BY-NC 2.5)

het invoeren van een Enterprise Privacy Management Systeem (EPMS). Een eerste belangrijke stap daarbij is het vastleggen van het privacybeleid, in eerste instantie op een hoog niveau. Dit beleid wordt vervolgens uitgewerkt in gedetailleerde regels die voor elk type informatie aangeven welke operaties op die informatie mogen worden uitgevoerd, door wie, en onder welke condities. Daarnaast wordt geïnventariseerd binnen welke bedrijfsprocessen op dit moment persoonsgegevens worden verwerkt en of er wordt voldaan aan deze regels. Het EPMS kan dit deels automatisch doen, op basis van een formele beschrijving van deze processen. Ook wordt gecontroleerd of bepaalde noodzakelijke processen (zoals de mogelijkheid tot inzage) afdoende zijn geïmplementeerd. Vaak zullen IT-systemen moeten worden aangepast en moeten controls worden ingebouwd om naleving van de regels af te dwingen. Ook hierin kan het EPMS een belangrijke rol spelen, als centrale repository van het privacybeleid en de daaruit afgeleide regels.

Soms is het privacy management systeem (PMS) gecombineerd met het information security management systeem (ISMS) tot een geïntegreerd geheel. Dat kan kostenbesparend zijn, maar draagt ook een zeker risico in zich mee. Omdat ISMS'en al langer worden gebruikt, kan het er toe leiden dat privacy vooral in termen van security wordt gezien en geïmplementeerd. Of erger nog, dat privacy ondergeschikt wordt gemaakt aan security. Het moge duidelijk zijn dat privacy en security slechts deels overlappen qua doelstellingen en bijbehorende maatregelen.

Hebben deze bedrijven überhaupt nagedacht over de verwerking van persoonsgegevens?

Daarnaast zouden bedrijven ook online inzage in de persoonsgegevens van een klant kunnen bieden, zoals Google dat al deels met haar Dashboard doet, en zoals bepaalde webwinkels ook de aankoopgeschiedenis online tonen. Inzage wordt zo een primair proces. Voor consumenten is dit natuurlijk zeer gebruikersvriendelijk. Er schuilt hier echter wel een groot risico in. Ook kwaadwillenden hebben zo, in theorie, simpel toegang tot andermans persoonsgegevens. Zo raken we, qua privacy, van de regen in de drup.

Een dergelijke vorm van online inzage vraagt dus om een voldoende veilige vorm van authenticatie, om er zeker van te zijn dat het de klant zelf is die inzage in zijn gegevens vraagt. Gebruikersnaam en wachtwoord is hier niet altijd veilig genoeg voor. Denk bijvoorbeeld aan het Elektronisch Patiënten Dossier, financiële gegevens, of gegevens uit juridische dossiers. Voor inzage in dergelijke systemen is een sterkere vorm van authenticatie noodzakelijk. Een landelijke betrouwbare identiteitsinfrastructuur ontbreekt hiervoor op dit moment echter. DigiD is niet betrouwbaar genoeg, en systemen die op dit moment worden gebruikt voor internetbankieren zijn niet toepasbaar in andere sectoren.

Dit is meteen een interessant voorbeeld van het wellicht ironische feit dat soms een sterke vorm van authenticatie van *jouw* identiteit juist nodig is om je privacy te beschermen. De andere kant op ligt dat meer voor de hand. Een opsporingsambtenaar moet zich kunnen identificeren voordat je verplicht bent zelf je paspoort of rijbewijs te tonen. Sterke authenticatie van websites (door middel van TLS) is een ander voorbeeld van een maatregel die er voor bedoeld is om te voorkomen dat jouw persoonlijke gegevens in verkeerde handen vallen. Maar dat terzijde.

Soms is een sterke vorm van authenticatie juist nodig om privacy te beschermen

Volgend jaar testen we het recht op inzage nog een keer. Laten we er samen voor zorgen dat de bedrijven en organisaties in Nederland dan beter scoren.