



Onderzoek meldplicht persoonsgegevens

Dr. Sieuwert van Otterloo
IT-expert bij SoftwareZaken
Amsterdam, 7 juli 2015
otterloo@gmail.com

Managementsamenvatting

Privacy is een zeer belangrijk aspect bij online zakendoen, en grote bedrijven zijn daarom door de wet bescherming persoonsgegevens verplicht om zorgvuldig om te gaan met persoonsgegevens. Onder andere zij alle gegevens die ze verwerken melden bij een register gegevensverwerking. In dit onderzoek is gecontroleerd hoe zorgvuldig bedrijven met privacy omgaan door te controleren of en hoe ze gegevensverwerking melden in de praktijk.

In dit onderzoek zijn alle meldingen van de 25 bedrijven in de AEX-index geanalyseerd. Bij meer dan driekwart van de bedrijven zijn er problemen: onjuiste bedrijfsgegevens, incomplete, vage en ook overbodige meldingen. De conclusie is dat bedrijven te weinig aandacht besteden aan het goed informeren van gebruikers over privacy, en het CBP blijkbaar niet de mankracht heeft om de meldingen goed te kunnen controleren.

De volgende problemen zijn gevonden:

- Voor 3 van de 25 bedrijven zijn er helemaal geen meldingen
- Organisatienamen en plaatsen staan niet goed in register
- Er ontbreken veel meldingen
- Meldingen zijn vaag en incompleet
- Er worden overbodige meldingen gedaan
- Het is niet te zien of meldingen nog actueel zijn
- Het register is niet doorzoekbaar op thema of datum

Waarschijnlijk voldoen veel bedrijven, groot en klein, niet aan de regels voor gegevensverwerking. Het advies aan deze bedrijven is om zich beter te verdiepen in de regels en binnen het bedrijf mensen aan te stellen en op te leiden op het gebied van privacy en informatiebeveiliging. Waarschijnlijk speelt er ook een gebrek aan samenwerking tussen verschillende afdelingen: de IT-ers kennen de meldplicht niet, en de juristen weten niet goed welke gegevens worden verzameld. Het advies in dit geval is om de juridische afdeling, de marketing afdeling en de IT-afdeling meer samen te laten werken aan privacy en beveiliging. Het aanstellen van een speciale functionaris gegevensbescherming, vanaf volgend jaar verplicht voor grote bedrijven, kan hierbij helpen.

Doel van het onderzoek

Digitale privacy is een belangrijk grondrecht voor iedereen. Dit recht is op verschillende manieren beschermd door wetten en regels, die ook regelmatig aangescherpt worden. In Nederland gaat het bijvoorbeeld om de Wet Bescherming Persoonsgegevens (WBP), maar ook de cookie-wet van een aantal jaar geleden, de meldplicht datalekken die in juni 2015 is goedgekeurd door de eerste kamer en binnenkort ingaat. Ook is er een nieuwe Europese verordening voor privacy, die waarschijnlijk in 2016 ingaat.

In deze wetten worden bedrijven die persoonsgegevens hebben een aantal verplichtingen opgelegd. De belangrijkste eisen zijn beschreven in de handleiding wet bescherming persoonsgegevens:

1. Bedrijven moeten voor alle gegevens die ze hebben nagaan of het op enige manier terug te leiden is tot personen. Zo ja, dan zijn het persoonsgegevens.
2. Bedrijven mogen persoonsgegevens alleen met toestemming, voor specifieke doelen verzamelen
3. Bedrijven moeten melden bij het CBP dat ze persoonsgegevens verwerken
4. Bedrijven moeten de persoonsgegevens beveiligen
5. Bedrijven moeten de personen over wie het gaat inzage geven en het recht op correctie of verwijdering

In de praktijk is het moeilijk om na te gaan hoe bedrijven met deze regels omgaan op al deze aspecten. In het nieuws komen alleen de negatieve verhalen en incidenten en hieruit ontstaat geen compleet beeld. Het doel van het onderzoek is om door middel van een steekproef op 25 bedrijven na te gaan in hoeverre bedrijven goed omgaan met digitale privacy. We focussen op onderdeel 3, het melden van gegevensverwerking. Dit punt is namelijk goed te onderzoeken door gebruik te maken van het register van meldingen dat via <https://cbpweb.nl> te raadplegen is.

Scope van het onderzoek

Er is voor gekozen om de 25 bedrijven uit de AEX-index te onderzoeken. Dit zijn allemaal grote bedrijven waarvan het waarschijnlijk is dat zijn aan gegevensverwerking doen. Ook zijn deze bedrijven goed verspreid over verschillende sectoren. In de tabel hieronder zijn de bedrijven weergegeven, inclusief de gebruikte zoekwoorden en het aantal gevonden meldingen.

Beursgenoteerd bedrijf	Gezocht op	aantal meldingen
Royal Dutch Shell	Shell	50
Koninklijke Philips Electronics	Philips	40
ING Groep	ING Amsterdam	30
Unilever	Unilever	24
Koninklijke DSM	DSM	20
Heineken	Heineken	20
Nationale nederlanden	Nationale-Nederlanden	12
AkzoNobel	Akzo	10
Delta Lloyd Groep	Delta Lloyd	10
Randstad	Randstad	10
TNT Express	TNT	9

Koninklijke KPN	KPN	6
Wolters Kluwer	Kluwer	6
AEGON	Aegon	5
Reed Elsevier	Elsevier	5
Koninklijke Vopak	Vopak	5
ASML Holding	ASML	4
Koninklijke Ahold	Ahold	2
ArcelorMittal	Arcelor	2
Unibail-Rodamco	Rodamco	2
Aalberts Industries	Aalberts	1
Gemalto	Gemalto	1
Altice	Altice	0
Boskalis	Boskalis	0
OCI	OCI	0

Bij meer dan dertig meldingen is er sprake van een schatting. Het exact tellen is lastig omdat er vaak sprake is van meerdere bedrijven waarvoor dezelfde melding is gedaan.

NB: Dit onderzoek is niet bedoeld als kritiek op de specifieke bedrijven: de bedrijven zijn slechts gekozen als voorbeeld.

Resultaten

Uitkomsten 1: Dubbele voorkomens

Een groot praktisch probleem bij het gebruik van het register is het dubbel vermeld staan van bedrijven. Wie zoekt op een bedrijfsnaam krijgt meerdere resultaten. In principe is dit bedoeld voor bedrijfsgroepen met meerdere deelbedrijven. In de praktijk blijkt echter dat veel bedrijven hun eigen naam of standplaats niet correct invoeren, en dat het register niet goed wordt gecontroleerd. Hierdoor zijn er veel dubbele vermeldingen, zoals hieronder weergegeven als voorbeeld bij Shell.

19 Shell International B.V.		's-gravenhage
20 Shell International B.V.	's-gravenhage	
21 Shell International B.V.	den haag	
22 Shell International B.V.	den haag	den haag
23 Shell International BV		's-gravenhage

In de tabel hieronder is weergegeven hoeveel resultaten er zijn, en ook hoeveel daarvan dubbel zijn.

Beursgenoteerd bedrijf	aantal BV's en NV's	Dubbele organisaties	percentage dubbel
ING Groep (ING Amsterdam)	28	16	57%
Koninklijke Philips Electronics	26	15	58%
Nationale-Nederlanden	11	5	45%
Royal Dutch Shell	49	14	29%
AkzoNobel	49	12	24%

Unilever	12	4	33%
Koninklijke DSM	9	3	33%
AEGON	3	2	67%
Koninklijke KPN	4	2	50%
TNT Express	6	2	33%
Heineken	8	2	25%
Randstad	24	2	8%
Wolters Kluwer	4	1	25%
Delta Lloyd Groep	6	1	17%
ArcelorMittal	9	1	11%
Aalberts Industries	1	0	0%
Koninklijke Ahold	1	0	0%
ASML Holding	2	0	0%
Gemalto	1	0	0%
Reed Elsevier	1	0	0%
Unibail-Rodamco	2	0	0%
Koninklijke Vopak	5	0	0%

Uitkomsten 2: soorten meldingen

Hieronder is een top 10 gemaakt van de meest gemelde soorten gegevensverwerking. Het gaat in veel gevallen om voor de hand liggende soorten verwerking, passend bij normale bedrijven.

1. Personeelszaken
2. Beveiligingscamera's
3. Toegangscontrole
4. whistleblower regeling
5. Opties en aandelen voor topmanagement
6. incidentenregister
7. Sollicitanten
8. Marketing
9. telefoon, portofoon en email-monitoring
10. zakelijke uitgaven en credit cards

Opvallend zijn de meldingen van opties en aandelen voor topmanagement, en de whistleblower-regeling (klokkenluidersregeling). Dit zijn heel juridische onderwerpen die ook over hele kleine groepen mensen gaan: waarschijnlijk tien per jaar of minder. Waarschijnlijk zijn deze kleine bewerkingen wel gemeld omdat hier goede juristen bij betrokken zijn die de wet goed kennen. De veel grotere marketing-gegevensbestanden worden vervolgens weer niet gemeld, waarschijnlijk omdat de juridische afdeling hier niet bij betrokken is. Het is jammer dat de privacy van topmanagers beter gerespecteerd wordt dan die van consumenten. In de tabel hieronder is per bedrijf aangegeven wat de belangrijkste aangetroffen meldingen zijn. De tabel is niet compleet: raadpleeg hiervoor het register zelf.

Beursgenoteerd bedrijf	Aangetroffen meldingen
Aalberts Industries	Verstrekken van gegevens aan kopers van nieuwbouwwoningen
AEGON	incidentenregister, pensioen
Koninklijke Ahold	executive option plan

AkzoNobel	klokkenluidersregeling (7 delen), bezoekersregistratie
Altice	geen
ArcelorMittal	aandelenplan voor werknemers, whistleblower regeling
ASML Holding	insider trading rules, speakup gedragscodes, gezondheidsonderzoeken
Boskalis	geen
Delta Lloyd Groep	panel', belangstellenden, incidentenregister, helpdesk-ondersteuning
Koninklijke DSM	portofoon, cameratoezicht, personeels en salarisadministratie, arbodienst, sollicitanten
Gemalto	videobeelden
Heineken	klanten/gebruikers, sollicitanten, active directory
ING Groep (ING Amsterdam)	juridische dienstverlening, vragen DNB, atlas, incidentenregister, marketingactiviteiten
Koninklijke KPN	klanten/gebruikers, medewerkers, camera
NN Group	Incidenten, gebeurtenissen, clientgegevens, aangaan en uitvoeren overeenkomsten
OCI	geen
Koninklijke Philips Electronics	job-application, bloedbank, toegangscontrole, applicatie-onderhoud, executive compensation,
Randstad	uitzendkrachten, kandidaten, pre-employment screening
Reed Elsevier	relatiebeheer, e-discovery
Royal Dutch Shell	opslag alle email, gezichtenboek, credit card, frauderende-medewerkers
TNT Express	contractafhandeling, call monitoring, personeelsadministratie
Unibail-Rodamco	beveiligingscamera's, mac-adressen tellen
Unilever	personeelsadministratie, camera, deskundigen, straatvoetbaltoernooi life and cooking consumentendatabase
Koninklijke Vopak	toegangscontrole, portofoon, camerabewaking
Wolters Kluwer	office suite

Uitkomsten 3: Bevindingen

Ook bij de meldingen die wel in het register zijn, zijn er veel onduidelijkheden. Hieronder hebben we er een aantal opgesomd:

Vage en onduidelijke omschrijvingen

Bij verschillende meldingen is er sprake van hele algemene en nietszeggende omschrijvingen. Bijvoorbeeld:

- Bij Delta Lloyd, melding 1401315, panel: er wordt gesproken over “achtergrondgegevens”, zonder verdere toelichting. Het doe is “segmentatie”, ook zonder toelichting
- Unilever heeft een melding ‘remedy’ gedaan, nummer 1222051. Het doel van deze melding is “verbeteren van de Unilever dienstverlening van HR Nederland”: een zeer breed doel dat voor elk veld is ingevuld. Het is niet duidelijk hoe het doel samenhangt met de gegevens
- Een andere melding met onduidelijke doelstelling is nr. 1347656 van Philips International. Het doel van de verwerking is “verbeteren van efficiency, kost control, benchmarking en organisatie-analyse en ontwikkeling”. Dit zijn heel

algemene doelen die waarschijnlijk voor het hele bedrijf gelden. Er wordt niet toegelicht waarom men voor cost control persoonsgegevens nodig heeft.

- Reed Elsevier verwerkt gegevens van abonnees, ex-abonnees en potentiële abonnees. Dit is een zeer brede groep waaronder men iedereen zou kunnen scharen. Het zou beter zijn als Elsevier de gegevens van ex-abonnees weggooit in plaats van blijft bewaren.

Onbekende verwerkers

Ook frustrerend is het feit dat sommige meldingen, onder andere bij een melding van Philips, als ontvangende partij alleen “medewerkers van bewerker” invullen. Dit is een nietszeggende mededeling. Iemand die het register raadpleegt doet dit omdat hij/zij juist wil weten wie de bewerkers zijn.

Overbodige meldingen

Het CBP meldt in de handleiding van de wet bescherming persoonsgegevens het volgende:

Van veel gegevensverwerkingen is algemeen bekend dat zij plaatsvinden en is het onwaarschijnlijk dat de persoonlijke levenssfeer van de betrokkenen door die verwerking wordt geschaad. Denk bijvoorbeeld aan een personeels- of ledenadministratie. De wetgever acht het niet nodig dat ook al die standaard- gegevensverwerkingen worden gemeld.

(bron: handleiding wet bescherming persoonsgegevens¹, pagina 32)

Het valt op dat veel bedrijven dit blijkbaar niet gelezen hebben, en wel algemeen bekende handelingen opslaan. Het gaat bijvoorbeeld om:

- HR zaken en salarisadministratie
- Active directory (een normaal IT-systeem)
- Pensioen
- Toegangscontrole
- Sollicitanten

Het register wordt niet overzichtelijker met dit soort meldingen. Als bedrijven dit soort activiteiten toch melden, zouden ze moeten toelichten wat er dan bijzonder is aan de verwerking. Het CBP zou vervolgens moeten filteren en alleen de niet algemeen bekende handelingen moeten opnemen.

Actualiteit

Bij het gebruik van het register valt op dat er niet is aangegeven wanneer een melding is gedaan, en of de melding nog is gecontroleerd of bijgewerkt. Dit zorgt voor onduidelijkheid: wanneer is men begonnen met bijhouden, en gebeurt het nog? Hoe langer het register blijft bestaan, hoe harder dit nodig.

Een voorbeeld waarbij dit relevant is, is bijvoorbeeld de melding van Unilever voor een straatvoetbaltoernooi. Op zich is het goed voorstelbaar dat Unilever rond het toernooi zelf een administratie nodig had. Het is echter niet te zien wanneer dit toernooi was, en of Unilever de gegevens nog steeds bewaard voor eventuele senioren-toernooien.

Zoekuitdagingen

Een ander zoekprobleem betreft het zoeken rond thema. Unibail-Rodamco heeft bijvoorbeeld aangegeven dat zij telefoons herkennen op basis van mac-adres om bezoekers te tellen. Goed dat dit gemeld is en op bedrijfsnaam makkelijk te vinden. Het is helaas niet mogelijk om op onderwerp te zoeken of op gebied.

¹ <http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html>

Conclusies en aanbevelingen

Bij dit onderzoek is gekeken naar 1 belangrijk aspect van privacywetgeving: de meldplicht van bedrijven om gegevensbewerking aan te melden. Uit het onderzoek blijkt dat bedrijven privacy nog onvoldoende serieus nemen. Bedrijven lijken niet op de hoogte van de wettelijke verplichtingen rond melding en lijken er onvoldoende moeite in te steken.

We vermoeden dat bedrijven die de meldplicht persoonsgegevens niet goed kennen, ook de andere wetten niet goed kennen. We raden elk bedrijf aan de laatste wetgeving goed te bestuderen en het beleid op orde te brengen. Er komt nieuwe wetgeving aan waarin de boetes omhoog gaan. Elk bedrijf zal in 2015 moeten zorgen om de gegevensbescherming echt op orde te brengen om incidenten, boetes en reputatieschade te voorkomen.

De uitdaging voor veel bedrijven is dat de benodigde kennis over privacy en gegevensbescherming verspreid is over de IT-afdeling en de juridische afdeling. Het advies aan deze bedrijven is om de afdelingen meer samen te laten. Ook moeten alle mensen die hier bij betrokken zijn meer kennis opdoen over het onderwerp gegevensbescherming, zodat zij persoonsgegevens herkennen en zowel de juridische als technische aspecten kennen.

Naast aanbevelingen aan de bedrijven, hebben we in het onderzoek ook een aantal verbeterpunten voor het CBP geconstateerd: ten eerste om meldingen beter te gaan controleren op met name bedrijfsgegevens. Hiermee worden de dubbele meldingen voorkomen. Daarnaast zouden er meer zoekmogelijkheden moeten komen en zou er ook een datum van aanmelding en van laatste wijziging vermeld moeten worden.

Achtergrond

Over de auteur:



Dr. Sieuwert van Otterloo is een allround IT-expert die zaken bekijkt vanuit technisch, bedrijfskundig en juridisch perspectief. Sieuwert van Otterloo heeft wiskunde en kunstmatige intelligentie gestudeerd en is gepromoveerd in de informatica. Sinds 2005 is hij managementconsultant: eerst bij McKinsey&Company, later bij de Software Improvement Group en vervolgens als oprichter van SoftwareZaken.

Sieuwert van Otterloo heeft veel interesse in technologie-strategie en heeft zich daarom verdiept in technologie-startups: hij is investeerder in verschillende startups en interviewt veel startups. In 2012 richtte hij StartupJuncture op, het grootste Engelstalige blog over Nederlands startups.

Om zijn technische en juridische kennis op peil te houden heeft Sieuwert de juridische opleiding Gerechtelijk Deskundige gedaan. Ook is hij lid van de NVBI, het NGFG en toegelaten tot de deskundigen-registers van SGOA en LRGD.

In 2014 heeft Sieuwert van Otterloo het ICT Institute mede-opgericht: een nieuw initiatief om de kennis vanuit SoftwareZaken ook in te zetten bij grote internationale bedrijven.

Over SoftwareZaken:

Softwarezaken is een onafhankelijk adviesbureau voor inzicht in IT. Het doel is te zorgen dat IT op de juiste manier wordt ingezet. Hiervoor deelt SoftwareZaken kennis, geeft workshops en training en doet onderzoek. De organisatie van SoftwareZaken bestaat uit een kernteam van vier IT-specialisten met samen meer dan veertig jaar academische en praktische ervaring in de IT.

SoftwareZaken geeft verschillende trainingen over het onderwerp digitale privacy en gegevensverwerking, bijvoorbeeld gericht op secure coding, functionarissen gegevensbescherming of cyber resilience.

Voor deze trainingen en ons advies werken we samen met andere partijen, bijvoorbeeld IT-advocaten en security-onderzoekers en maken we gebruik van al zoveel mogelijk open beschikbare informatie. We komen graag in contact met andere personen met expertise op dit onderwerp, zoals IT-advocaten en security-onderzoekers.

Dankwoord

Voor dit rapport hebben gebruik gemaakt van kennis en materiaal van onder andere Solv advocaten, CBP, visuelevoorwaarden.nl, <http://www.iusmentis.com>, zebralegal.com en projectmoore.com. We willen al deze partijen danken voor hun hulp.

Meer informatie

Voor vragen en opmerkingen, neem contact op via www.softwarezaken.nl of www.ictinstitute.nl (Engelstalig).

Bron titel-afbeelding: pixabay – OpenClipartVectors – creative commons