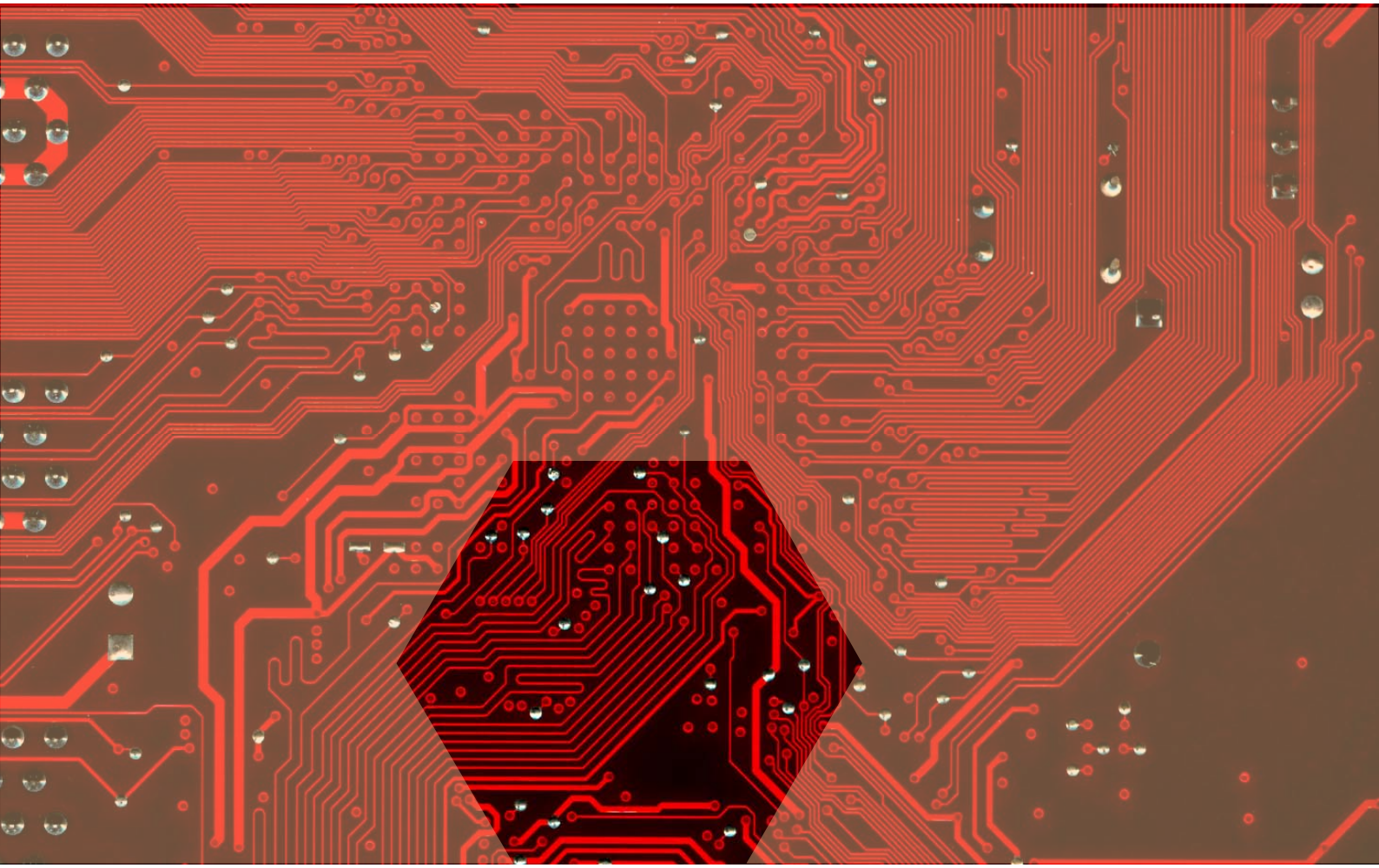
Research voor Beleid
onderdeel van Panteia



Melding maken?

Internationale quick scan meldplicht gegevensverlies

Eindrapport

Een onderzoek in opdracht van het Ministerie van Economische Zaken

drs. L. Boer
drs. T.K. Grimmius

B3477

Zoetermeer, 27 januari 2009

Voorwoord

Dit rapport doet verslag van een onderzoek naar de wijze waarop in het buitenland organisaties die aan hen toevertrouwde persoonsgegevens verliezen, melding van dit verlies moeten maken aan betrokkenen. Het onderzoek, dat is uitgevoerd in opdracht van het ministerie van Economische Zaken, beoogt inzicht te bieden in discussies over en ervaringen met deze melding in het buitenland en zo aanknopingspunten te geven voor de mogelijke invoering van een meldplicht in Nederland.

Ten behoeve van het onderzoek, dat is uitgevoerd in de periode van september tot en met december 2008, is deskresearch gedaan en zijn interviews gehouden met vertegenwoordigers van overheden en toezichthouders in het buitenland en met enkele Nederlandse stakeholders en deskundigen. Een deel van de interviews met buitenlandse respondenten is afgenomen door onze collega Judith Zweers. Wij danken de respondenten hartelijk voor hun medewerking.

Het onderzoek is begeleid door een commissie bestaande uit Peter Hondebrink (MinEZ), Carlo Luyten (MinBZK), Jan Timmermans (MinBZK), Daniel Tijink (MinEZ), Roman Volf (MinEZ) en Anja van Zantvoort (MinJus). We zeggen de commissie dank voor de plezierige en constructieve samenwerking.

Lisanne Boer
Ton Grimmius

Inhoudsopgave

Samenvatting 8

Deel I Onderzoeksopzet en bevindingen 17

1 Vraagstelling en onderzoeksopzet 19
- 1.1 Beleidscontext 19
- 1.2 Doel- en vraagstelling 20
- 1.3 Onderzoeksopzet 21
- 1.4 Leeswijzer 21

2 Gegevens en gegevensverlies: waar hebben we het over? 23
- 2.1 Persoonsgegevens 23
- 2.2 Gegevensbeherende organisaties en diensten van de informatiemaatschappij 23
- 2.3 Gegevensverlies 24
- 2.4 Schade door gegevensverlies 26

3 Selectie landen en introductie case-studies 27
- 3.1 Selectie landen 27
- 3.2 Landen met meldplicht 28
- 3.3 Landen met vrijwillige melding 32
- 3.4 Landen met discussie over mogelijke invoering meldplicht 34

4 Resultaten quick scan 37
- 4.1 De meldplicht in theorie 37
- 4.2 Elementen van meldingen 38
- 4.3 Discussie: argumenten voor en tegen 40
- 4.4 Bevindingen 41
- 4.5 Is een meldplicht effectief? Gebrek aan empirische gegevens 53

5 Vormgeving meldplicht in Nederland 55
- 5.1 2005: Discussie komt op gang 55
- 5.2 Vormgeving meldplicht in Nederland: meningen van experts 56
- 5.3 Belangrijkste aandachtspunten voor Nederland samengevat 61

Deel II Case-studies 63

Case-studies: landen met meldplicht 65

6 Breach laws op federaal niveau 67

7 *Breach laws* in deelstaten 73

8 Californië 77

9 Nevada 83
10 Noorwegen 87

Case-studies: landen met vrijwillige melding 91
11 Canada 93
12 Australië 97

Case-studies: discussie over mogelijke invoering meldplicht 101
13 Europese Unie 103
14 Duitsland 111
15 Verenigd Koninkrijk 115

Bijlage 1 Overzicht respondenten 119

Bijlage 2 Checklist interviews buitenland 121

Bijlage 3 Checklist interviews Nederland 123

Samenvatting

1. Doelstelling en onderzoeksopzet

Doelstelling

Mede als gevolg van recente incidenten in het buitenland waarbij door overheidsorganisaties en bedrijven beheerde privacygevoelige persoonsgegevens op straat kwamen te liggen, is in Nederland steeds meer de vraag aan de orde of, naar Amerikaans voorbeeld, een meldplicht zou moeten worden ingevoerd die organisaties verplicht gegevensverlies te melden. Ook de op handen zijnde herziening van de Europese richtlijn 2002/58/EC[1] maakt deze vraag actueel: in de nieuwe richtlijn is een meldplicht voorzien voor telecomaanbieders en *internet service providers* (ISP's)[2].

Per brief van 10 juli 2008 aan de Tweede Kamer kondigde de minister van Binnenlandse Zaken en Koninkrijksrelaties een onderzoek aan naar de vormgeving van en ervaringen met meldplicht in het buitenland. Dit sluit aan bij de eerdere toezegging uit 2005 van het kabinet aan de Tweede Kamer, op grond waarvan de minister van Economische Zaken een onderzoek naar de meldplicht heeft geëntameerd. Onderhavig onderzoek, dat in opdracht van het ministerie van Economische Zaken is uitgevoerd, geeft invulling aan de in de brief van de minister van Binnenlandse Zaken en Koninkrijkrelaties in 2008 aangekondigde inventarisatie. Doel van het onderzoek is de situatie en ervaringen met een meldplicht in het buitenland te inventariseren teneinde aandachtspunten te formuleren die van belang zijn voor de Nederlandse discussie en de vormgeving van een eventuele meldplicht in Nederland.

Door de recente datum waarop andere landen de meldplicht hebben ingevoerd en het daardoor geconstateerde gebrek aan empirische gegevens over de effecten van een meldplicht, heeft het onderzoek niet geresulteerd in een evidence-based overzicht van aanbevelingen voor de vormgeving van een meldplicht. Bovendien zijn dit soort keuzen over de vormgeving afhankelijk van de nationale context (visie, juridisch stelsel, samenwerking overheid-bedrijfsleven, etc.). Het onderzoek heeft een overzicht opgeleverd van de elementen die moeten worden ingevuld bij de vormgeving van een meldplicht (zie 4 hieronder), de wijze waarop dit in andere landen is gebeurd en de overwegingen die daarbij zijn gehanteerd. Tot slot is onder enkele Nederlandse experts onderzocht hoe volgens hen de meldplicht in Nederland zou moeten worden vormgegeven.

Onderzoeksopzet

Het onderzoek heeft het karakter van een quick scan en omvat in de eerste plaats een inventarisatie van de situatie en ervaringen in andere landen. Deze inventarisatie is gedaan door deskresearch en telefonische interviews met overheidsfunctionarissen. Om een zo

[1] Volledige titel: Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[2] Momenteel verschillen de Europese Commissie en de Telecomraad enerzijds en het Europees Parlement anderzijds van mening over de doelgroep van de meldplicht. In het voorstel van de EC en de Raad geldt de voor telecomaanbieders en internet service providers (ISP's); het Europees Parlement stelt een meldplicht voor voor alle diensten van de informatiemaatschappij.

breed mogelijk beeld te krijgen, is het onderzoek niet beperkt tot landen met een meldplicht. De volgende landen zijn geselecteerd:

- *Landen met een wettelijke meldplicht*: Verenigde Staten en Noorwegen.
  Naast een inventarisatie van de meldplicht in federale wetgeving in de Verenigde Staten is een algemeen beeld verkregen van de meldplicht op deelstaatniveau. Twee deelstaten, te weten Californië en Nevada, zijn nader onderzocht.
- *Landen met vrijwillige melding*: Australië en Canada.
- *Landen waar discussie is over mogelijke invoering van een meldplicht:* Duitsland, het Verenigd Koninkrijk. Tevens zijn de plannen van de Europese Unie op dit gebied nader onderzocht.

In de tweede plaats zijn enkele Nederlandse experts geïnterviewd over de wenselijkheid van een Nederlandse meldplicht en de vormgeving daarvan.

In het vervolg van deze samenvatting gaan we achtereenvolgens in op:

- de in de discussies over het al dan niet invoeren van een meldplicht gehanteerde argumenten;
- motieven om een meldsysteem in te voeren;
- de elementen van een meldsysteem en de daarin door verschillende landen gemaakte keuzen;
- de effectiviteit van meldsystemen.

De mening van de geïnterviewde Nederlandse experts wordt tevens behandeld.

2. Argumenten voor en tegen de meldplicht

Onderstaande tabel geeft een overzicht van de in het onderzoek geïnventariseerde argumenten voor en tegen een meldplicht.

Voor	Tegen
Burgers hebben er recht op te weten dat hun persoonsgegevens gevaar lopen; Als burgers op de hoogte zijn van een veiligheidsinbreuk, kunnen zij tijdig maatregelen treffen om schade te voorkomen; Burgers herwinnen het vertrouwen in organisaties als deze inbreuken melden en burgers op de hoogte stellen van de maatregelen die de organisatie neemt om schade en toekomstige inbreuken te voorkomen; Een meldplicht is een stimulans voor bedrijven om meer aandacht aan de beveiliging van persoonsgegevens te schenken en deze te verbeteren om zo de imagoschade, administratieve lasten, kosten en sancties te voorkomen die met een melding gepaard gaan; Door melding te verplichten komen overheden en organisaties meer te weten over aantallen en de aard van data breaches, zodat: - de overheid de regulering kan verbeteren; - toezichthouders bedrijven en organisaties beter kunnen begeleiden bij het omgaan met veiligheidsinbreuken en het verbeteren van de beveiliging; - organisaties hun beveiliging kunnen verbeteren.	(Overvloedige) melding van veiligheidsinbreuken maakt burgers: - angstig en nodeloos ongerust, want slechts een klein deel van alle veiligheidsinbreuken leidt tot identiteitsfraude; - onverschillig voor meldingen en niet meer bereid reageren op de serieuze gevallen; Uit angst voor imagoschade na melding van een veiligheidsinbreuk, zullen organisaties deze juist intern willen houden; De procedure van melding brengt hoge kosten en administratieve lasten voor bedrijven met zich mee; De private sector heeft de beveiliging al goed op orde: een meldplicht is niet nodig; Preventie en verbetering van veiligheidsmaatregelen verdienen de voorkeur boven een meldplicht; Een meldplicht levert problemen op met aansprakelijkheid; omdat het vaak onduidelijk is wie de dader is en hoe en waar een veiligheidsinbreuk heeft plaatsgevonden, is het niet duidelijk wie voor de kosten van een melding moet opdraaien; De financiële crisis heeft het vertrouwen in banken van de consument al geschaad; door banken te verplichten veiligheidsinbreuken te melden, neemt dit vertrouwen nog verder af.

3. Motivaties voor de invoering van een meldsysteem

In geen van de in het onderzoek betrokken landen waren voor de invoering van een meldsysteem dan wel de discussie over de invoering daarvan betrouwbare gegevens bekend over gegevensverlies en de gevolgen daarvan. Een belangrijk motief om een meldsysteem in te voeren dan wel de discussie daarover te starten zijn incidenten waarbij gegevens zijn verloren en/of het toenemende aantal klachten van burgers over misbruik van hun persoonsgegevens. Dataschandalen in de Verenigde Staten en het Verenigd Koninkrijk liggen mede ten grondslag aan het besluit van Australië en Canada een meldsysteem in te voeren.

4. Elementen van een meldsysteem

Uit het onderzoek komt naar voren dat bij de invoering van een meldsysteem besluitvorming omtrent de volgende elementen aan de orde is:

- doel van het meldsysteem
- verplichte of vrijwillige melding?
- doelgroep: welke organisaties zijn meldplichtig?
- soort gegevens: op welke gegevens is de meldplicht van toepassing?
- grondslag voor melding: wanneer melden?
- aan wie melden?
- handhaving en toezicht: wie is verantwoordelijk voor de handhaving en welke instrumenten heeft de toezichthouder ter beschikking?
- wettelijke verankering.

Ten aanzien van al deze elementen moeten keuzen worden gemaakt. Deze keuzen bepalen de uiteindelijke vormgeving van een systeem. Hieronder gaan we kort in op de verschillende elementen.

Doel van het meldsysteem

Een meldplicht is doorgaans gericht op het voorkomen van schade voor burgers door veiligheidsinbreuken bij organisaties die over privacygevoelige gegevens over hen beschikken.

De vraag is dan hoe een meldplicht bijdraagt aan de realisatie van deze doelstelling. Uit het onderzoek komt naar voren dat de relatie tussen een meldplicht enerzijds en het te bereiken hoofddoel anderzijds, in theorie verloopt via drie sporen.

1 De meldplicht spoort gegevensbeherende organisaties aan hun beveiliging te optimaliseren omdat ze met een meldplicht gepaard gaande kosten en/of imagoschade willen voorkomen.
2 De meldplicht versterkt het toezicht en de handhaving doordat inzicht wordt verkregen in de aard en risico's van veiligheidslekken.
3 De meldplicht versterkt de positie van de burger. Zo is hij mogelijk in staat na een melding maatregelen te nemen om de gevolgen van het verlies van zijn gegevens te beperken. Ook kan hij bij het kiezen van organisaties om zaken mee te doen rekening houden met hun reputatie op het gebied van gegevensbeheer.

In de Verenigde Staten wordt met de meldplicht in de eerste plaats ingezet op het eerste spoor. De verwachting is dat organisaties de beveiliging van hun databases optimaliseren, teneinde imagoschade als gevolg van het moeten melden van gegevensverlies te voorkomen. In de tweede plaats moet de meldplicht burgers in staat stellen maatregelen te nemen tegen verlies van hun gegevens, bijvoorbeeld het tijdig blokkeren van creditcards of doordat de meldplicht het de burgers mogelijk maakt te procederen tegen organisaties die hun gegevens zijn kwijtgeraakt. Dit laatste hangt samen met het ontbreken van een overkoepelende privacywetgeving en toezicht in het Amerikaanse rechtssysteem.

Ook in andere onderzochte landen is de stimulans die van een meldsysteem uitgaat voor bedrijven om hun systemen optimaal te beveiligen een belangrijke argument voor invoering van een dergelijk systeem. In Noorwegen, Australië en Canada heeft het systeem ook duidelijk ten doel de toezichthouder beter te informeren over de mate waarin veiligheidsinbreuken

voorkomen en de aard van de inbreuken. Deze kennis moet hem in staat stellen bedrijven beter te kunnen voorlichten en adviseren over hoe veiligheidsinbreuken te voorkomen.
De Nederlandse respondenten zijn van mening dat van een meldplicht vooral een stimulans voor bedrijven uitgaat om gegevensverlies te voorkomen. Daarnaast hechten zij veel waarde aan toezicht en handhaving met een nadruk op sanctioneren (zie verder Handhaving en toezicht). Volgens de respondenten is het instellen van een meldsysteem met als doel burgers in staat te stellen maatregelen te nemen om schade te voorkomen niet erg effectief. In de praktijk zijn er voor burgers weinig middelen beschikbaar om de schade te beperken. Gegevensverlies komt immers vaak juist aan het licht nadat al schade is geleden. Wel is het volgens de respondenten van belang dat er een instantie is waar burgers terecht kunnen met vragen over wat te doen na een melding dat ze (mogelijk) zijn getroffen door gegevensverlies.

Flankerend beleid
Enkele Nederlandse respondenten stellen dat invoering van een meldplicht gepaard zou moeten gaan met flankerend beleid:

- Oprichting centrale instantie waar slachtoffers van identiteitsfraude terecht kunnen door bijvoorbeeld het bestaande agentschap van het ministerie van BZK te verstevigen door overheidsbrede samenwerking;
- Introductie 'fraudeer-mij-niet' register naar voorbeeld van o.a. het CIFAS-register in het Verenigd Koninkrijk;
- Instellen klokkenluiderregeling of het aanstellen van een interne privacy commissaris bij organisaties;
- Uitbreiding van de opsporingscapaciteit van hackers bij de politie;
- Uitbreiding van de handhaving/toezicht capaciteit bij de OPTA.

Verplichte of vrijwillige melding?
Doorgaans is de melding verplicht of gaan de gedachten uit naar een verplichte melding. Een uitzondering hierop vormen Australië, Nieuw-Zeeland en Canada. In Australië is de melding (vooralsnog) vrijwillig omdat de overheid in nauwe samenwerking met het bedrijfsleven wil komen tot een meldplicht die draagvlak heeft onder het bedrijfsleven. Canada streeft ernaar de huidige vrijwillige melding te vervangen door een verplichting.

Doelgroep
De Amerikaanse deelstaten en de nationale overheden van andere landen hebben veelal gekozen voor een meldplicht voor *alle* organisaties die binnen de grenzen van de staat *werkzaam* zijn. Hierbij wordt geen onderscheid gemaakt tussen het bedrijfsleven en (semi-)overheid. In enkele deelstaten in de Verenigde Staten geldt de meldplicht alleen voor de private sector.

Door de afwezigheid van overkoepelende privacy wetgeving, is op federaal niveau in de Verenigde Staten alleen voor een aantal *sectoren* en *organisaties* een meldplicht van toepassing. Binnen de Europese Unie is de doelgroep van de op handen zijnde meldplicht een belangrijk punt van discussie. De Europese Commissie en de Telecomraad willen de meldplicht beperken tot de telecomsector; het Europees Parlement heeft de voorkeur voor een meldplicht die verder gaat en voor alle diensten van de informatiemaatschappij geldt.

De Nederlandse respondenten hebben een voorkeur voor een meldplicht die geldt voor zowel de overheid als het bedrijfsleven. Sommige experts betwijfelen of organisaties hun beveiliging naar aanleiding van de meldplicht willen en kunnen aanscherpen. Respondenten verwachten dat met name kleine bedrijven niet kapitaalkrachtig genoeg zijn om te investeren in beveiliging. Ook denken ze dat organisaties zich – om sancties en imagoschade te voorkomen – niet altijd aan de meldplicht zullen houden.

Soort gegevens

De meldplicht ziet op het verlies van '*persoonsgegevens*'. In de Verenigde Staten worden met deze term gewoonlijk gegevens bedoeld waarmee een individu kan worden geïdentificeerd. In een aantal andere landen, waaronder Australië, Duitsland en Noorwegen, is de definitie breder. Hier geldt de meldplicht voor 'gevoelige' persoonsgegevens gerelateerd aan de persoonlijke levenssfeer (politieke, religieuze, seksuele voorkeuren etc).

De meldplicht kan ook worden afgebakend op grond van de *drager* waarop de persoonsgegevens zijn opgeslagen. In de meeste landen is de meldplicht alleen van toepassing op digitale gegevens. In Australië is men van mening dat de meldplicht zo breed mogelijk moet zijn en niet beperkt tot digitale gegevens.

Bijna zonder uitzondering kiezen deelstaten in de Verenigde Staten ervoor *versleutelde* gegevens uit te sluiten van de meldplicht. Er wordt vanuit gegaan dat het risico op schade kleiner is als de gegevens zijn versleuteld. Daarnaast wordt verondersteld dat deze beperking van de meldplicht organisaties stimuleert hun gegevens te beveiligen.

Grondslag voor melding

De grondslag moet voorkomen dat burgers en/of toezichthouders overspoeld worden met meldingen. Ook kan een heldere afbakening van te melden incidenten administratieve lasten en kosten voor gegevensbeherende organisaties beperken. Het bepalen van deze grondslag voor melding blijkt een van de meest lastige beslissingen bij de vormgeving van een meldplicht. Uit het onderzoek kwam een aantal mogelijke grondslagen naar voren:

1 melding van *alle* veiligheidsinbreuken (zonder dat is aangetoond dat een onbevoegde daadwerkelijk gegevens heeft verkregen)
2 onbevoegde *toegang* tot persoonsgegevens (idem)
3 persoonsgegevens *verkregen* door onbevoegde
4 risico op *misbruik* of onrechtmatige *verspreiding* van persoonsgegevens
5 risico op *schade* voor betrokkenen
6 a*antal* verloren gegevens of gedupeerden.

De grondslagen verkrijgen van persoonsgegevens ('acquisition of data') en het risico op (een vorm van) schade voor betrokkenen worden het meest toegepast. Onder 'schade' wordt in de Verenigde Staten meestal financiële schade verstaan. In andere landen schaart men er ook imagoschade en andere vormen van schade in relatie tot de persoonlijke levenssfeer onder. Het aantal verloren gegevens of gedupeerden wordt vrijwel nooit als grondslag gebruikt; het verlies van creditcardgegevens kan voor één persoon immers al erg schadelijk zijn.

Over wanneer zou moeten worden gemeld hebben Nederlandse respondenten in het algemeen nog geen uitgekristalliseerde ideeën. Eén van hen vindt dat gemeld moet worden na-

dat is gebleken dat onbevoegden toegang hebben gehad tot een systeem met persoonsgegevens, zonder dat aangetoond behoeft te zijn dat deze gegevens ook daadwerkelijk zijn gestolen. Een ander zou de grondslag willen leggen bij een minimum aantal verloren gegevens. Alleen bij een ernstige inbreuk zou moeten worden gemeld.

Aan wie melden?
De meldplicht vereist in alle landen in ieder geval melding aan de getroffen personen wier persoonsgegevens gevaar lopen als gevolg van een veiligheidsinbreuk. Het is ook mogelijk dat een organisatie een veiligheidsinbreuk eerst moet melden aan een toezichthouder. Samen wordt dan bepaald of melding aan burgers nodig is. Dit is het geval in een aantal Amerikaanse deelstaten. Ook in de Australische en Europese voorstellen voor een meldplicht wordt deze procedure toegepast.

Binnen de Europese Unie wordt momenteel overleg gevoerd tussen het Europees Parlement, de Europese Commissie en de Raad over voorstellen voor een meldplicht binnen de Europese telecomwetgeving. Het *Europees Parlement* stelt de volgende procedure voor:
Stap 1: melding van 'alle veiligheidsinbreuken' aan de toezichthouder
Stap 2: in geval van *imminent and direct danger* melding aan de betrokkenen. Of melding aan betrokkenen nodig is, bepaalt de toezichthouder. De organisatie kan ook zelf besluiten meteen aan betrokkenen te melden.
Stap 3: jaarlijkse rapportage van alle veiligheidsinbreuken betrokkenen.
De *Europese Commissie* en de *Raad* stellen in reactie voor dat dienstaanbieders in alle gevallen *zelf* bepalen of een veiligheidsinbreuk aan de betrokkenen moet worden gemeld. Uit de reactie van enkele respondenten blijkt verder dat er nog geen eenduidigheid bestaat over de betekenis die de Europese Commissie en het Europees Parlement aan de formulering 'alle veiligheidsinbreuken' hechten.

Handhaving en toezicht
In de Verenigde Staten vindt in principe geen actieve handhaving plaats. Dit land kent geen centrale toezichthouder die de privacy wetgeving handhaaft, zoals de landen in Europa en Canada en Australië. In de Verenigde Staten is de Attorney General of District Attorney vaak verantwoordelijk voor handhaving van de meldplicht; in andere landen is dit de nationale toezichthouder.

Een aantal landen legt bij de handhaving de nadruk op *sanctionering*, zoals de Verenigde Staten en het Verenigd Koninkrijk. Toegepaste sanctie-instrumenten zijn een boete, publicatie, aanspannen van rechtszaken en verplichte audits bij vermoeden van niet-navolging. Australië en Noorwegen zien meer in handhaving op basis van *co-operatie en communicatie*. De nadruk ligt op het geven van voorlichting over het omgaan met veiligheidsinbreuken. In Duitsland wordt een *combinatie* van sanctioneren en co-operatie overwogen.

In landen met discussie over de invoering van een meldplicht is de capaciteit van de toezichthouders een belangrijk aandachtspunt.

Omdat zij niet verwachten dat organisaties zich altijd aan de meldplicht houden, hechten de Nederlandse respondenten veel belang aan toezicht en handhaving door sanctioneren. Volgens hen hangt de keuze voor de toezichthouder af van de vormgeving van de meldplicht:
- wanneer de doelgroep van de meldplicht wordt beperkt tot telecomsector: OPTA

- wanneer de meldplicht van toepassing is op meerdere doelgroepen:
  - CBP
  - Samenwerking OPTA en CBP
  - Toezichthouder per sector: OPTA, DNB en andere sectorale toezichthouders
  - Toezicht door Justitie: Openbaar Ministerie, parket-generaal, staatsbeveiligingsorganisatie

De geïnterviewde Nederlandse experts verschillen van mening over de rol van de toezichthouder. Enerzijds is opgemerkt dat de toezichthouder niet alleen een adviserende rol dient te hebben, maar moet kunnen handhaven. Een respondent prefereert samenwerking tussen toezichthouder en het bedrijfsleven.

Evenals in het buitenland, is in de interviews met de Nederlandse deskundigen verschillende malen gewezen op het belang dat de toezichthouder over voldoende capaciteit beschikt om de meldplicht te handhaven. De benodigde capaciteit is voor een belangrijk deel afhankelijk van de reikwijdte en de grondslag van de meldplicht.

Handhavingsinstrumenten
Nederlandse experts noemen de volgende instrumenten om de meldplicht te handhaven:
- Boetebevoegdheid toezichthouder
- Naming & shaming achteraf door toezichthouder in geval van niet-melden
- Verplichte EDP-audits door forensische accountants / toezichthouder

De meningen over het nut en de noodzaak van een boete zijn verdeeld.

Wettelijk kader
De keuze voor het wettelijk kader waarbinnen een meldplicht wordt opgenomen is voor een deel afhankelijk van de staatsstructuur van een land. Omdat een overkoepelende privacy wet in de Verenigde Staten ontbreekt, heeft de federale overheid in de Verenigde Staten een meldplicht opgenomen in een aantal sectorale wetten. De Amerikaanse deelstaten kennen een meldplicht die is vastgelegd in overkoepelende wetgeving of in een aparte wet. Een aantal landen, te weten Australië, Duitsland en Noorwegen, heeft de herziening van hun privacy wetgeving aangegrepen om een meldplicht in te voeren dan wel te overwegen. Zoals eerder opgemerkt stelt de Europese Unie voor om een meldplicht op te nemen in de Europese telecomregelgeving.

In Nederland kan de meldplicht in verschillende wetten worden ingekaderd. Genoemde mogelijkheden zijn de Telecommunicatiewet, de Wet Bescherming Persoonsgegevens en de Wet Economische Delicten.

5. Is een meldplicht effectief? Gebrek aan empirische gegevens

De literatuur biedt onvoldoende (gefundeerd) inzicht in de effectiviteit van de meldplicht, omdat landen die een meldsysteem kennen deze recent ingevoerd hebben. Ook onze gesprekspartners beschikken niet over harde gegevens. Er is niet empirisch aangetoond dat een meldplicht bijdraagt aan het voorkomen of een afname van veiligheidsinbreuken of

schade voor burgers[1]. Evenmin is onderzocht in welke mate een melding angst, wantrouwen of juist vertrouwen wekt bij burgers. Tenslotte is onbekend in hoeverre de meldplicht wordt nageleefd.

Een aantal respondenten denkt dat sinds de invoering van de meldplicht gegevensbeherende organisaties meer aandacht besteden aan de beveiliging van hun systemen. Een Amerikaanse respondent leidt dit af uit de stijgende uitgaven voor encryptie-software en een toenemend aantal congressen over gegevensbeveiliging. Zoals hierboven aangegeven: een causale relatie is volgens respondenten echter niet aangetoond. Andere respondenten vermoeden dat ondanks een meldplicht veel veiligheidsinbreuken niet worden gemeld.

Volgens de geïnterviewde Nederlandse experts heeft een meldplicht alleen effect als het sluitstuk is van een omvattende systematiek die duidelijke eisen bevat voor het beveiligen van systemen met persoonsgegevens. Als de kwaliteit van de beveiliging van persoonsgegevens goed is, wordt ook schade voor burgers verkleind.

[1] Tijdens het onderzoek kwam één recente studie aan het licht, waarin wordt gesteld dat de invoering van een meldplicht 'a marginal effect' heeft op de afname van identiteitsfraude. Volgens deze studie is het aantal incidenten er met 'just under 2%, on average' door gereduceerd. Bron: Carnegie Mellon University, Do Data Breach Disclosure Laws Reduce Identity Theft? (September, 2008).

Deel I Onderzoeksopzet en bevindingen

1 Vraagstelling en onderzoeksopzet

Dit rapport doet verslag van een internationaal onderzoek naar verplichtingen voor organisaties om melding te maken van verlies van door hen beheerde persoonsgegevens. Gelet op incidenten met gegevensverlies in onder andere de Verenigde Staten en het Verenigd Koninkrijk is het ministerie van Economische Zaken geïnteresseerd in een verkenning van opgedane ervaringen met wetgeving die melding van veiligheidsinbreuken verplicht. Hiermee komt de minister tegemoet aan de eerdere toezegging van het kabinet uit 2005. Het onderzoek past tevens in de toezegging van de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) onderzoek te doen naar een meldplicht in verschillende landen. De aldus verkregen inzichten zullen als input dienen voor de verdere discussies in Nederland.

1.1 Beleidscontext

Tijdens het Algemeen Overleg in de Tweede Kamer van 3 april 2008 over de bescherming van de vitale infrastructuur, stelde de PvdA voor grote bedrijven te verplichten hackpogingen te melden.[1] Doel hiervan is meer grip te krijgen op de terroristische bedreigingen van de vitale infrastructuur, die voor 80% in handen is van publieke partijen[2]. Al eerder, in 2005, vroeg de SP in het kader van de aanpassing van de Wet Computercriminaliteit om de invoering van een meldplicht voor bedrijven, overheden en andere organisaties die gegevens van burgers verliezen.

Op Europees niveau wordt gewerkt aan een voorstel voor een meldplicht in geval van gegevensverlies. Het betreft een herziening van de richtlijn 2002-58-EG. De aanleiding voor de wijziging van deze richtlijn is de in 2002 voorgenomen hervorming van de telecommunicatiesector teneinde de Europese interne telecommunicatiemarkt te voltooien.[3] Het voorstel houdt in dat aanbieders van elektronische communicatiediensten bepaalde veiligheidsinbreuken (verplicht) moeten melden aan de nationale autoriteiten. Het doel hiervan is:

' (…) to enhance the protection of personal data and the privacy of individuals in the electronic communications sector, in particular, by strengthening security-related provisions and enforcement mechanisms.' [4]

In opdracht van het ministerie van Economische Zaken (EZ) wordt een verkennend onderzoek uitgevoerd naar de mogelijkheid een meldplicht in te voeren voor bedrijven en/of overheden indien sprake is van verlies van privacygevoelige gegevens. De minister van BZK zegde tijdens het kamerdebat van 3 april 2008 toe "een internationale inventarisatie te la-

[1] Verslag Algemeen Overleg, Tweede Kamer, vergaderjaar 2007–2008, 29 668 en 26 643, nr. 21

[2] De bescherming van de vitale infrastructuur maakt deel uit van het nationale veiligheidsbeleid. 'Vitale infrastructuur' is een verzamelterm voor 12 vitale sectoren en 33 bedrijven waarvan het uitvallen 'maatschappelijke ontwrichting' kan veroorzaken. Het gaat bijvoorbeeld om banken, de voedselsector, transport en de telecomsector.

[3] Advies Europees Economisch en Sociaal Comité over voorstellen herziening Europese telecomwetgeving (TEN/327-329, Brussel, 29 mei 2008), p. 4.

[4] Article 29 Data Protection Working Party, Opinion on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive) (00989/08/EN, WP150, Adopted on 15 May 2008) p. 2.

ten verrichten met betrekking tot een meldplicht voor vitale bedrijven in geval van hackpogingen." Per brief van 10 juli 2008[1] herhaalt ze deze toezegging en wijst ze op het Europese voorstel.

1.2 Doel- en vraagstelling

Onderhavig onderzoek geeft invulling aan het door de minister in haar brief aan de Tweede Kamer aangekondigde inventarisatie en aan de toezegging uit 2005. Volgens deze brief heeft het onderzoek een tweeledige doelstelling:

- "een beeld krijgen van de situatie en ervaringen in andere landen
- lering trekken uit de ervaringen met de invoering van een meldplicht"[2] (in andere landen)."

Om een zo breed mogelijk beeld te krijgen van de situatie en ervaringen in andere landen, hebben we het onderzoek niet beperkt tot landen met een meldplicht. Immers, ook discussies en argumenten in landen die overwegen een meldplicht in te voeren en van landen die er bewust voor hebben gekozen van een meldplicht af te zien, kunnen inzichten bieden die van belang zijn voor de Nederlandse besluitvorming.

We hebben daarom a-priori drie typen landen onderscheiden.

- Landen met een wettelijke meldplicht of een vrijwillige melding (naast de doorgaans verplichte meldingen zijn er landen met een systeem van vrijwillige meldingen)
- Landen waarin discussie plaatsvindt over mogelijke invoering van een meldsysteem
- Landen die er bewust voor hebben gekozen van een meldsysteem af te zien.

Uiteindelijk hebben we niet een land kunnen vinden dat bewust heeft afgezien van een meldsysteem. Deze categorie komt dan ook in dit rapport verder niet ter sprake.

Op grond van het voorafgaande liggen de volgende vragen ten grondslag aan het onderzoek.

A. Landen met een wettelijke of vrijwillige melding

1 Wat is de aanleiding geweest een meldsysteem in te voeren?
2 Wat waren argumenten voor en tegen invoering van een meldsysteem?
3 Hoe is de meldplicht vormgegeven en wat waren de overwegingen daarbij?
4 Hoe wordt de melding gehandhaafd?
5 Is er inzicht in de effecten van het meldsysteem; zo ja welke effecten zijn er? Wat zijn voor en nadelen?

B. Landen waar invoering van een meldsysteem in discussie is

6 Waarom wordt invoering van een meldsysteem overwogen?
7 Wat zijn argumenten voor en tegen de invoering?
8 Voor zover daar zicht op is: hoe wordt de melding vormgegeven en wat zijn de overwegingen daarbij?
9 Voor zover daar zicht op is: hoe wordt het systeem gehandhaafd?

[1] Brief van de minister van BZK, Tweede Kamer, vergaderjaar 2007–2008, 29 668 en 26 643, nr. 22.
[2] Idem.

C. Leerpunten

10 Welke leerpunten zijn af te leiden uit de ervaringen met het meldsysteem?

1.3 Onderzoeksopzet

Het onderzoek heeft de opzet van een quick scan die tot doel heeft de onderzoeksvragen op hoofdlijnen te beantwoorden. Met name een verdieping van de landenstudies zou een uitgebreider onderzoek vragen.

Voor zover het het buitenland betreft, is de quick scan beperkt tot bestudering van het *overheidsperspectief* op de invoering van wetgeving voor het melden van veiligheidsinbreuken en gegevensverlies[1]. Per land zijn respondenten benaderd die werkzaam zijn bij relevante overheidsorganisaties. In Nederland heeft de studie zich vooral gericht op inhoudelijke deskundigen op het gebied van identiteitsfraude, internetveiligheid, informatiestrategie en media- en telecommunicatierecht. Ook zijn toezichthouders CBP en OPTA en de VNO-NCW als respondenten bij het onderzoek betrokken. Een overzicht van alle respondenten is opgenomen bijlage 1.

Het onderzoek bestaat uit de volgende onderdelen.

1 Deskresearch naar landen met een verplichte dan wel vrijwillige melding en landen waar discussie is over het al dan niet invoeren van een meldplicht. De deskresearch was er op gericht de onderzoeksvragen zoveel mogelijk te beantwoorden.
2 Telefonische interviews met overheden/toezichthouders in een aantal – in overleg met de begeleidingscommissie gekozen - landen om de resultaten van de deskresearch te verdiepen. De checklist voor deze interviews is opgenomen in bijlage 2.
3 Interviews met Nederlandse deskundigen en stakeholders (voor de checklist, zie bijlage 3).

1.4 Leeswijzer

Het vervolg van het rapport is als volgt opgebouwd.

- Hoofdstuk 2 gaat in op een aantal voor het onderzoek van belang zijnde begrippen.
- Hoofdstuk 3 geeft een overzicht van de landen waarop het onderzoek zich heeft gericht en een korte typering van de bevindingen over deze landen. In Deel II van het rapport zijn de diverse landenstudies meer in detail beschreven.
- Hoofdstuk 4 bevat de bevindingen van de quick scan en gaat in op de aan het onderzoek te ontlenen leerpunten voor de Nederlandse situatie.

[1] Volledigheidshalve: in het onderzoek in het buitenland zijn bedrijven en instellingen buiten beschouwing gebleven.

2 Gegevens en gegevensverlies: waar hebben we het over?

2.1 Persoonsgegevens

In dit onderzoek naar melding van gegevensverlies gaat het om persoonsgegevens. Een persoonsgegeven is in de Wet Bescherming Persoonsgegevens gedefinieerd als: “elk gegeven betreffende een geïdentificeerde of identificeerbare persoon”.[1]

Persoonsgegevens verschaffen *direct* of *indirect* informatie over een individu. Gegevens als naam, geboortedatum en adres verschaffen bij koppeling aan een individu direct informatie over dat individu. Gegevens over andere personen of objecten kunnen ook indirect informatie verschaffen over een individu. Het ministerie van Justitie geeft op haar website als voorbeeld de winst van een eenmanszaak en de waarde van een auto[2]. Als dergelijke gegevens zijn te herleiden tot de eigenaar van de zaak of auto geven ze informatie over diens inkomenspositie. Ook in dit geval gaat het om persoonsgegevens.

Persoonsgegevens zijn dus te koppelen aan individuele identificeerbare personen. Een code op een lijst bij het ministerie van OCW dat het onderwijsniveau aangeeft voor een leerling-nummer zegt op zichzelf niets totdat het via het leerling-nummer wordt gekoppeld aan identificatiegegevens (bijvoorbeeld naam, adres e.d.) van de betreffende leerling.

2.2 Gegevensbeherende organisaties en diensten van de informatiemaatschappij

Vele organisaties beschikken over persoonsgegevens. Te denken valt aan overheidsorganisaties (bijvoorbeeld Belastingdienst, IB-groep, Gemeentelijke Basisadministratie), zorg- en medische instellingen, onderwijsinstellingen, bedrijven (klantgegevens), werkgevers (personeelsgegevens), etc. Persoonsgegevens zijn tegenwoordig doorgaans digitaal opgeslagen in databases.

Door de digitalisering van gegevens en met name de elektronische uitwisseling van gegevens spelen telecommunicatie-en ICT-bedrijven een belangrijke rol. Ze zijn niet slechts beheerder van gegevens van hun klanten en personeel, maar vooral ook de schakel die elektronische uitwisseling van gegevens tussen burgers en organisaties en tussen organisaties onderling mogelijk maken. Deze telecommunicatie- en ICT-sector biedt internet- en telefonische netwerken aan waarmee de burger toegang krijgt tot diensten als internetbankieren, overheidsdiensten, ‘ínternetwinkels’, zoekmachines en communicatienetwerken als Hyves en LinkedIn. Dergelijke diensten worden aangeduid als ‘diensten van de informatiemaatschappij’.

[1] Wet Bescherming Persoonsgegevens, art. 1a.
[2] www.minjus.nl

Diensten van de informatiemaatschappij

Het Burgerlijk Wetboek (art. 3:15d lid 3) verstaat onder diensten van de informatiemaatschappij: "elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn."

De zinsnede "tegen vergoeding" wordt breed opgevat. Naast diensten waarbij online overeenkomsten worden gesloten, vallen hier ook activiteiten onder als het gratis aanbieden van online informatie of het ter beschikking stellen van zoekfaciliteiten op het internet, indien het gaat om activiteiten waarvoor doorgaans wel wordt betaald of die anderszins een zekere waarde in het economisch verkeer vertegenwoordigen.

Voorbeelden:

- e-commerce sites (Wehkamp.nl, Bol.com)
- internetbankieren
- gratis diensten (on-linedagbladen, forums, Facebook, Hyves, MySpace)
- online ontspanning (YouTube, online games, virtuele museumbezoeken)
- technische diensten die als tussenpersoon optreden (het verschaffen van toegang tot een communicatienetwerk, web hosting, elektronisch berichtenverkeer)
- certificeringsdiensten (elektronische archivering, aangetekende verzending, tijdsregistratie en handtekening),
- online zorgproviders
- telefoonboeken en zoekmachines (Google)

Bronnen: www.ejure.nl, Internet Observatory[1], Europees Parlement[2]

2.3 Gegevensverlies

Onder gegevensverlies, in het Engels 'data breach', is te verstaan dat *bij een organisatie opgeslagen persoonsgegevens in handen van een onbevoegde derde partij zijn gekomen*[3]. Zoals we in de hoofdstukken hierna zien, gaan sommige meldplichten verder dan het daadwerkelijke verlies van gegevens. Dit, omdat het voorkomt dat duidelijk is dat onbevoegden zich weliswaar toegang hebben verschaft tot een systeem met persoonsgegevens, maar niet of ze daadwerkelijk toegang tot deze gegevens zelf hebben gehad. Niet het feitelijke, aantoonbare verlies van persoonsgegevens is dan de grondslag voor de meldplicht, maar het mogelijke verlies van gegevens doordat onbevoegde derden toegang hebben gehad tot het systeem waarin deze gegevens zijn opgeslagen.

[1] Internet Observatory: Démoulin, M., Hervé, J., Bespreking van de wetten betreffende diensten van de informatiemaatschappij (CRID, 2003) Website: http://www.internet-observatory.be/internet_observatory/pdf/legislation/cmt/law_be_2003-03-11_cmt_nl.pdf

[2] Website Europees Parlement, Artikel: Telecoms: better services for consumers and a safer internet (24 september 2008) Website: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20080924+ITEMS+DOC+XML+V0//EN&language=EN#sdocta13

[3] Hierbij past de kanttekening dat 'verlies' niet inhoudt dat de gegevens niet meer in het bezit zijn van de organisatie, maar dat een ongeautoriseerde partij er toegang tot heeft gekregen en de gegevens heeft kunnen kopiëren.

Er zijn verschillende manieren om onbevoegd toegang te verkrijgen tot systemen met persoonsgegevens en deze gegevens zelf. In hoofdlijnen gaat het om *diefstal* doordat onbevoegden zich onrechtmatig toegang hebben verschaft tot de database van een gegevensbeheerder en om *verlies* door de gegevensbeheerder zelf[1].

Diefstal
Een populaire vorm van diefstal is *hacking*. In de Verenigde Staten deed Verizon onderzoek naar ruim 500 data breaches in de periode 2004 – 2007.[2] Bij ruim de helft (59%) bleek, naast mogelijke andere oorzaken, sprake te zijn van hacking. Een andere belangrijke vorm van diefstal is het installeren van malafide software of *malcode* (malicious code). Verizon berekende dat *malcode* ten grondslag lag aan eenderde van de 500 onderzochte cases[3]. Andere vormen van diefstal zijn het installeren van botnets, het verspreiden van computervirussen, het zich toegang verschaffen tot een systeem met een valse identiteit of het stelen van fysieke media als laptops, cd-roms en memorysticks. Diefstal wordt niet alleen gepleegd door externen, maar ook personeelsleden, partnerorganisaties of subcontractors kunnen zich op niet legitieme wijze meester maken van persoonsgegevens.

Verlies
Naast diefstal zijn fouten (van medewerkers) van gegevensbeherende organisaties een belangrijke oorzaak voor het onbedoeld beschikbaar komen van persoonsgegevens voor onbevoegde derden. In de eerste plaats moet worden gedacht aan wat Verizon 'error' noemt. Dit gaat om fouten die zijn gerelateerd aan het systeembeheer, zoals onvoldoende besluitvorming over beveiliging, foute configuraties, 'omission' (systeembeheerder gaat er onterecht vanuit dat bepaalde veiligheidsmaatregelen actief zijn), niet-naleving van veiligheidsprocedures, storingen etc. 'Error' speelt een rol in 62% van de 500 door Verizon onderzochte inbreuken. In 3% van de gevallen leidden fouten tot het gevaarlopen van data, in 59% van de gevallen droegen ze er significant aan bij. In 79% van de errors is sprake van een 'omission'. Dit soort systeemgerelateerde fouten maken het voor inbrekers eenvoudiger een systeem binnen te dringen. Verizon denkt dat 87% van alle veiligheidsinbreuken voorkomen had kunnen worden door 'reasonable controls' .

Een andere bij de gegevensbeheerder gelegen oorzaak voor gegevensverlies is het kwijtraken van gegevensdragers als laptops, USB-sticks, CD-roms, papieren documenten etc. Denk bijvoorbeeld aan de recente incidenten van gegevensverlies in Groot-Brittannië en Duitsland.

[1] Hierbij past de kanttekening dat 'verlies' niet inhoudt dat de gegevens niet meer in het bezit zijn van de organisatie, maar dat een ongeautoriseerde partij er toegang tot heeft gekregen en de gegevens heeft kunnen kopiëren.
[2] Verizon Business RISK Tean, *2008 Data Breach Investigation Report: Four years of forensic research. More than 500 cases. One comprehensive report. (Verizon Business, 2008*).
[3] Malafide software wordt door de inbreker in de vorm van een virus, worm of *Trojan Horse* geïnstalleerd om data te vernietigen, hem in staat te stellen in te breken in het systeem of toegang te krijgen tot data.

2.4 Schade door gegevensverlies

Burgers kunnen op verschillende manieren schade ondervinden van verlies van hun gegevens door een gegevensbeheerder.

- Financiële schade door verlies van creditcard- of pinpasgegevens, wachtwoorden en toegangscodes voor internetbankieren
- Imagoschade of chantage door het bekend worden van gevoelige informatie over bijvoorbeeld religieuze, politieke of seksuele voorkeur
- Fysieke schade, bijvoorbeeld diefstal of molest
- Identiteitsfraude, wanneer iemand anders zich voor de benadeelde burger uitgeeft. De fraudeur heeft niet alleen toegang tot diens gegevens maar kan ook op diens kosten goederen en diensten afnemen of zelfs criminele activiteiten ondernemen onder zijn slachtoffers naam. Identiteitsfraude 'kan overal en op velerlei manier plaatsvinden en is niet beperkt tot specifieke situaties, procedures of documenten'[1].

[1] Prof. Dr. Mr. J.H.A.M. Grijpink, Identiteitsfraude en overheid (Justitiële verkenningen, jrg. 32, nr. 7 2006)

3 Selectie landen en introductie case-studies

3.1 Selectie landen

Op basis van de deskresearch en in overleg met de begeleidingscommissie zijn in een aantal landen en deelstaten van de Verenigde Staten casestudies verricht (zie figuur 3.1). Deze landen zijn hieronder gecategoriseerd aan de hand van de in hoofdstuk 1 beschreven indeling in landen met meldplicht, landen met vrijwillige melding en landen waar discussie plaatsvindt over mogelijke invoering van een meldsysteem.

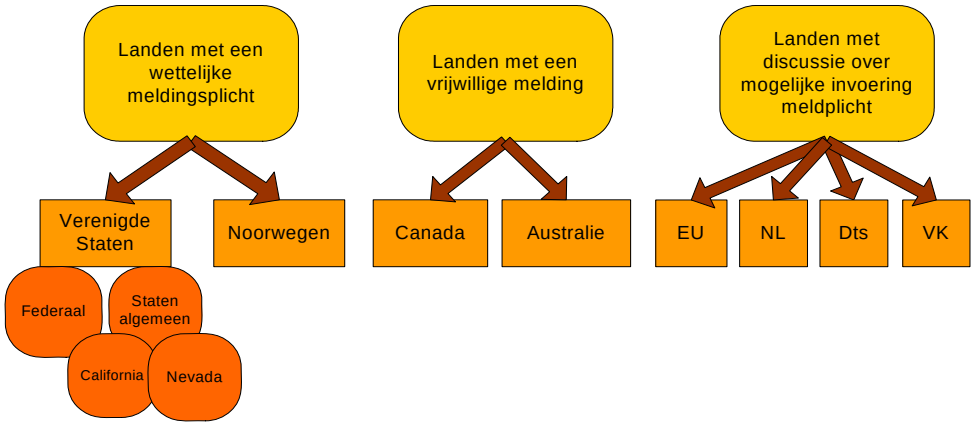
Landen met een wettelijke meldplicht
In de eerste plaats zijn de Verenigde Staten en Noorwegen geselecteerd. De Verenigde Staten is het eerste land dat een meldplicht invoerde, zowel op federaal niveau als op het niveau van de deelstaten. Noorwegen voerde als eerste en tot nog toe enige land in Europa een meldplicht in.

Naast een inventarisatie van de meldplicht in federale wetgeving in de Verenigde Staten is een algemeen beeld verkregen van de meldplicht op deelstaatniveau. In 44 van de 50 staten is een meldplicht ingevoerd. Twee deelstaten, te weten Californië en Nevada, zijn nader onderzocht. Deze staten verschillen in hun uitwerking van de meldplicht.

Landen met vrijwillige melding
In Australië, Nieuw Zeeland en Canada is sprake van een systeem van vrijwillige meldingen. Australië en Canada zijn als cases in het kader van dit onderzoek nader onderzocht.

Landen waar discussie is over mogelijke invoering van een meldplicht
In deze categorie vallen Duitsland, het Verenigd Koninkrijk en Nederland. Tevens zijn de plannen van de Europese Unie op dit gebied nader onderzocht.

Figuur 3.1 Overzicht uitgevoerde casestudies[1]



In de hoofdstukken van deel 2 van dit rapport zijn de diverse cases uitgebreid beschreven. In onderstaande paragrafen zijn ze kort samengevat.

3.2 Landen met meldplicht

De Verenigde Staten worden als voorloper gezien als het gaat om het invoeren van een verplichte melding van gegevensverlies. Het was het eerste land dat, op federaal niveau, een meldplicht implementeerde voor de financiële sector (1999). Een jaar later volgde Noorwegen, dat als eerste land in Europa een meldplicht invoerde.

In deze paragraaf worden de volgende casestudies behandeld:

- Verenigde Staten: federaal niveau
- Verenigde Staten: algemeen beeld meldplicht deelstaten
- Californië
- Nevada
- Noorwegen

[1] Deze selectie wijkt af van de oorspronkelijke selectie die ook Frankrijk, Zuid-Korea, Singapore en de Amerikaanse deelstaten Vermont, Indiana en North Carolina omvatte. Zuid-Korea en Singapore waren oorspronkelijk opgenomen omdat er binnen de begeleidingscommissie signalen waren dat in deze landen sprake is van een meldplicht. De contactpersonen voor deze landen en deelstaten bleken echter onbereikbaar (Zuid-Korea, Singapore en de Amerikaanse deelstaten) of achtten zich niet in de positie deel te nemen aan het onderzoek (Frankrijk). Op grond van laatstgenoemd argument weigerden ook Duitse en EU-contactpersonen deelname. In deze gevallen kon op grond van de bijdrage van andere respondenten en schriftelijke bronnen desalniettemin een dusdanig beeld worden verkregen dat Duitsland en de EU als casestudy gehandhaafd konden blijven. De casestudies Vermont, Indiana en North Carolina zijn vervangen door een algemene casestudy van meldplicht in 44 Amerikaanse deelstaten.

3.2.1 Verenigde Staten: federaal niveau

Om rekening mee te houden

Wanneer we de meldplicht in de Verenigde Staten vergelijken met (discussies over) een meldplicht in andere landen is het belangrijk rekening te houden met een aantal verschillen.

- *Federale staatsstructuur* In de Verenigde Staten bestaat zowel op federaal als staatsniveau wetgeving die melding van veiligheidsinbreuken verplicht. De wetgeving op federaal niveau kan verschillen van die van de staten; ook kan de meldplicht per staat andere elementen bevatten.
- *Andere privacy wetgeving* De meeste landen in Europa hebben de bescherming van privacy vastgelegd in een wet, waarin de ver-, bewerking en het beheer van persoonsgegevens wordt gereguleerd. In de VS is de bescherming van persoonsgegevens niet vastgelegd in een overkoepelende wet, maar in federale wetten van toepassing op een aantal sectoren.
- *Geen toezicht* De Verenigde Staten kent geen toezichthouder die de privacy wetgeving handhaaft, zoals de landen in Europa en Canada en Australië data of privacy autoriteiten kennen.

Op federaal niveau bestaat (nog) geen overkoepelende wet die de bescherming van alle soorten gevoelige persoonsgegevens voor zowel de overheid als het bedrijfsleven reguleert. De federale overheid hanteert een *sectorale* aanpak. Per sector zijn richtlijnen geïmplementeerd die bepaalde organisaties verplichten informatie goed te beveiligen. Het gaat om de financiële sector, gezondheidszorg, overheid, beveiliging- en internetsector. Een aantal van deze sectorale wetten bevat een meldplicht.

De onderliggende aanleiding voor het invoeren van een meldplicht was de toegenomen bezorgdheid over identiteitsfraude. Drie bekende wetten en richtlijnen met een meldplicht zijn:

- Gramm-Leach-Bliley Act (GLBA) uit 1999: de wet waarin voor het eerst een meldplicht werd opgenomen voor de financiële sector;
- Veterans Affairs Information Security Act uit 2007: voor de nationale veteranen organisatie;
- Office of Management and Budget Breach Notification Policy uit 2007: voor alle federale overheidsorganen.

Mogelijk wordt op federaal niveau alsnog een algemene meldplicht ingevoerd. Tot op heden is een dergelijke meldplicht nog niet tot stand gekomen, voornamelijk omdat men het niet eens kan worden over de criteria in welke gevallen gegevensverlies moet worden gemeld (in hoofdstuk 4 de grondslag voor melding genoemd). Daarnaast is de noodzaak voor een algemene meldplicht afgenomen nu 44 staten deze zelf al hebben ingevoerd. Een eventuele algemene meldplicht wordt niet geïmplementeerd door een overkoepelende nieuwe wet, maar door aanpassing van bestaande sectorale wetten.

3.2.2 Amerikaanse deelstaten algemeen

In de Verenigde Staten hebben sinds Californië in 2003 het voortouw nam in totaal 44 staten een meldplicht ingevoerd.

Aanleiding
Breach laws zijn gemotiveerd door toenemende bezorgdheid over identiteitsfraude. In de VS heeft invoering van een meldplicht door de deelstaat vaak tot doel om de gaten op te vullen waar geen federale meldplicht geldt.

Vormgeving
In de meeste staten in de Verenigde Staten geldt de meldplicht voor organisaties die binnen de grenzen van de staat *werkzaam* zijn[1]. Hierbij wordt geen onderscheid gemaakt tussen het bedrijfsleven en (semi-)overheid. In de meeste staten is de meldplicht alleen van toepassing op '*unencrypted, computerized*' persoonsgegevens. Er wordt vanuit gegaan dat het risico op schade kleiner is als de gegevens zijn versleuteld.

Deelstaten kiezen naar het voorbeeld van Californië meestal voor de grondslag *acquisition of data* (verkrijgen van data door onbevoegden) of een zekere vorm van (mogelijke) schade voor de betrokkenen. Enkele staten vereisen al melding zodra er een veiligheidsinbreuk heeft plaatsgevonden zonder dat daarbij aangetoond behoeft te zijn dat data zijn verkregen. De meeste deelstaten kiezen hier niet voor, voornamelijk omdat zij voorzien dat dit veel meldingen oplevert waardoor burgers nodeloos ongerust worden. Het aantal verloren gegevens of gedupeerden wordt vrijwel nooit als grondslag gebruikt; het verlies van creditcardgegevens kan voor één persoon immers al erg schadelijk zijn.

Handhaving
De Verenigde Staten heeft geen centrale toezichthouder die de privacy wetgeving handhaaft. Organisaties hoeven inbreuken dan ook meestal alleen aan de getroffen burgers te melden. Als een deelstaat er wel voor heeft gekozen de meldplicht te handhaven, is de District Attorney (Officier van Justitie) hiervoor verantwoordelijk. In een aantal staten hebben burgers het recht op basis van de meldplicht civiele procedures aan te spannen als zij slachtoffer zijn geworden van de gevolgen van een veiligheidsinbreuk. In gevallen dat dit niet mogelijk is kunnen ze juridische procedures aanspannen op basis van schending van wetgeving op gerelateerde terreinen als bescherming van consumenten, malpractice, fraude of oneerlijk handelen.

3.2.3 Californië

Aanleiding
Californië is de eerste staat in de Verenigde Staten die in 2003 een wettelijke meldplicht instelde. In de jaren voor de implementatie van de meldplicht had Californië reeds wetgeving ingevoerd met eisen aan beveiliging van persoonsgegevens. De directe aanleiding voor invoering van de meldplicht was een succesvolle inbreuk in de server van het data centrum van de staat begin 2002, het *Stephen P. Teale Data Center.*

Vormgeving
De meldplicht is van toepassing op *'Each agency, person, or business that conducts business in Californië and owns or licenses computerized data containing personal information'.*

[1] Security breaches chart Julie Brill, en overzicht Consumer's Union uit 2007.

De meldplicht voor bedrijven is in een andere wet opgenomen dan die voor overheidsorganisaties. Door een omissie geldt de plicht niet voor lokale overheden. Organisaties moeten melding maken aan de consument wanneer de organisatie weet dat een onbevoegd persoon niet-gecodeerde, geautomatiseerde persoonsgegevens heeft verworven, of dat hiertoe een reële mogelijkheid bestaat. Sinds 2008 vallen ook medische gegevens expliciet onder de meldplicht.

Handhaving
Naast Wisconsin heeft Californië als enige staat een *Office of Privacy Protection.* Dit bureau heeft geen handhavende bevoegdheden en dient voornamelijk als adviseur en beleidsmaker. Ook fungeert het *Office* in de praktijk als meldpunt voor bezorgde burgers.

3.2.4 Nevada

Aanleiding
De meldplicht in Nevada maakt deel uit van een wet die als doel heeft identiteitsfraude tegen te gaan. De onderliggende reden van de invoering van deze wet was een toename van het aantal arrestaties voor ID-fraude gerelateerde misdrijven in de staat.

Vormgeving
De vormgeving van Nevada's meldplicht komt sterk overeen met wetgeving op federaal niveau en in Californië. De meldplicht is van toepassing op *alle data collectors*: overheidsorganisaties, opleidingsinstituten, financiële instellingen, bedrijven en elke andere organisatie die 'handle, collect, disseminate or otherwise deal with non-public personal information'. Met name grote, commerciële instellingen worden als kwetsbaar gezien door hackers en zijn daarom vaak het doelwit van hackpogingen. Data collectors moeten betrokkenen op de hoogte stellen wanneer (een reële mogelijkheid bestaat dat) een onbevoegd persoon niet-versleutelde, digitale persoonsgegevens heeft verworven en wanneer is aangetoond dat (het redelijkerwijs mogelijk is dat) deze gegevens zijn misbruikt voor criminele doeleinden.

Handhaving
Nevada kent geen onafhankelijke toezichthouder. De meldplicht wordt achteraf gehandhaafd door de Attorney General (AG) of de District Attorney (DA). Wanneer de AG of DA van mening is dat een organisatie zich niet aan de wet houdt, kan hij een dwangbevel opleggen. De data collector zelf kan daarnaast via de rechtbank een schadevergoeding eisen van de degene die van de veiligheidsinbreuk heeft geprofiteerd. Volgens respondenten kan een meldplicht weinig effectief worden gehandhaafd, omdat het onwaarschijnlijk is dat de AG of DA als eerste achter een veiligheidsinbreuk komt.

3.2.5 Noorwegen

Aanleiding
De aanleiding voor het invoeren van de meldplicht als onderdeel van de privacy wetgeving in 2000 was de behoefte van de nationale toezichthouder, Datatilsynet, aan meer informatie over veiligheidsinbreuken bij organisaties. Met deze informatie wil Datatilsynet organisaties helpen met het verbeteren van beveiligingssystemen en -maatregelen.

Vormgeving
De meldplicht geldt voor alle data controllers die zijn gevestigd in Noorwegen en data controllers buiten de Europese economische zone die gebruik maken van 'equipment' in Noorwegen[1]. De plicht is van toepassing op gevoelige persoonsgegevens. De grondslag van melding zijn 'discrepanties in het veiligheidssysteem'. Hiermee wordt *'any use of the information system that is contrary to established routines and security breaches'* bedoeld. Organisaties dienen melding te maken aan de toezichthouder indien een 'discrepantie' kan leiden tot de onbevoegde openbaarmaking van persoonsgegevens.

Handhaving
De toezichthouder is verantwoordelijk voor de handhaving. Datatilsynet kan hiertoe inspecties uitvoeren en organisaties verplichten hun beveiliging te verbeteren. De toezichthouder publiceert zijn onderzoeken naar veiligheidsinbreuken op de website. Publicatie vindt pas plaats na overleg met de betreffende organisatie. Voorzover ons bekend kan de organisatie publicatie niet tegenhouden, maar biedt de mogelijkheid voor inzage organisaties wel een kans om publicatie te vertragen. Het niet opvolgen van eisen van Datatilsynet kan via de rechter leiden tot een boete, maar dit gebeurt in de praktijk zelden. De nadruk ligt op advies over de verbetering van veiligheidsmaatregelen en het onderhouden van een goede verstandhouding met organisaties.

3.3 Landen met vrijwillige melding

Voor zover ons bekend hebben Australië, Nieuw Zeeland en Canada een vrijwillige melding van veiligheidsinbreuken en gegevensverlies. In deze paragraaf gaan we nader in op de systemen van Canada en Australië.

3.3.1 Canada

Aanleiding
Op dit moment kent Canada nog geen meldplicht. Er geldt een aantal jaren een vrijwillige melding voor de private sector. In 2008 bracht de Privacy Commissioner een gids uit, waarin de vrijwillige melding staat beschreven[2]. Ook overheidsorganisaties kunnen veiligheidsinbreuken vrijwillig melden, maar dit is niet geformaliseerd. Een aantal provincies kent ook een vrijwillige melding voor de private sector. De Privacy Commissioner geeft echter de voorkeur aan een meldplicht, omdat de vrijwillige melding onvoldoende informatie over het aantal en de aard van veiligheidsinbreuken oplevert. De Canadese overheid bracht in April 2008 een voorstel uit voor een meldplicht voor de private sector en overheidsorganisaties[3].

Vormgeving
Het voorstel houdt het volgende in. Een veiligheidsinbreuk zou aan de toezichthouder en aan de betrokkenen moeten worden gemeld. De voorgestelde grondslag voor melding aan

[1] De Europese Unie plus Noorwegen, IJsland en Liechtenstein.
[2] Draft Voluntary Information Security Breach Notification Guide, April 2008: http://www.privacy.gov.au/publications/breach_0408.html#Voluntary
[3] Industry Canada, A model for data breach reporting and notification under PIPEDA (June 2008)

de toezichthouder is ‘material breaches’. De nadruk ligt hierbij op veiligheidsinbreuken waarbij de beveiligingsmaatregelen van een bedrijf, opzettelijk of onopzettelijk, worden doorbroken. Het bedrijfsleven zou niet bereid zijn zich achter een meldplicht te scharen die hen verplicht alle veiligheidsinbreuken te melden. De grondslag voor melding aan consumenten is ‘significant harm’. De meldplicht zou van toepassing worden op persoonsgegevens opgeslagen op alle soorten media, inclusief papier, bandopnamen en video. Ook het begrip ‘schade’ wordt breed opgevat: anders dan in veel staten in de Verenigde Staten, schaart Canada onder schade ook imagoschade en andere vormen van schade.

Handhaving
De Office of the Privacy Commissioner zou moeten toezien op de naleving van de meldplicht. Behalve de bevoegdheid om audits uit te voeren, aanbevelingen uit te brengen en naming & shaming toe te passen, heeft de toezichthouder momenteel geen handhavingsbevoegdheden. De toezichthouder ziet zich op dit moment geconfronteerd met een gebrek aan mankracht. Mogelijk beslist de regering de capaciteit van de toezichthouder uit te breiden.

3.3.2 Australië

Aanleiding
In de Australische privacy wetgeving, die op dit moment wordt herzien en naar verwachting over twee jaar wordt geïmplementeerd, wordt een meldplicht opgenomen. De Privacy Commissioner (toezichthouder) heeft in de zomer van 2008 vrijwillige melding geïntroduceerd bij wijze van voorbereiding op deze meldplicht[1]. Het Australische model is gebaseerd op de vrijwillige meldingen in Canada en Nieuw Zeeland. Het doel van de vrijwillige melding is het verzamelen van *best practices* en adviezen ter voorbereiding van de op handen zijnde meldplicht en het creëren van draagvlak.

Vormgeving
Het voorstel voor de meldplicht is op dit moment als volgt vormgegeven. Bedrijven en overheidsorganisaties zouden melding moeten maken aan de toezichthouder wanneer het verlies, onbevoegde toegang, gebruik, openbaarmaking, kopiëren of aanpassen van beveiligde persoonsgegevens (mogelijk) leidt tot ernstige schade voor betrokkenen. Het gaat niet alleen om digitale data, maar om persoonsgegevens in wat voor vorm dan ook. Samen met de organisatie zou de toezichthouder moeten bepalen of melding aan individuen nodig is.

Handhaving
De Privacy Commissioner is op dit moment verantwoordelijk voor de handhaving van de privacy wetgeving, en daarmee in de toekomst van de meldplicht. Om de wet te handhaven kan de Commissioner nu onderzoek en audits uitvoeren en (financiële) compensatie voor getroffenen eisen. Bij de vrijwillige melding ligt de nadruk op advisering en begeleiding van organisaties bij het omgaan met veiligheidsinbreuken. De toezichthouder heeft geen sanctiebevoegdheden: eventuele niet-naleving van besluiten moet worden aangepakt via de

[1] Office of the Privacy Commissioner: Guide to handling personal information security breaches

rechter. Mogelijk wordt er een boetebevoegdheid geïntroduceerd onder de herziene privacy wetgeving.

3.4 Landen met discussie over mogelijke invoering meldplicht

In Europa, zowel op het niveau van de Europese Unie als in de lidstaten, vindt momenteel discussie plaats over de mogelijke invoering van een meldplicht. Deze discussie verkeert in verschillende stadia. Binnen de Europese Unie liggen twee voorstellen voor een meldplicht in het kader van telecomwetgeving, waarover in het voorjaar van 2009 voor het laatst wordt gestemd. In Duitsland stemt de regering in december 2008 al over de invoering van een meldplicht. In het Verenigd Koninkrijk is de discussie in volle gang en wordt de invoering van de Europese meldplicht kritisch gevolgd. In Nederland verkeert de discussie over de meldplicht in het beginstadium.

Deze paragraaf bespreekt de discussies in:
- Europese Unie
- Duitsland
- Verenigd Koninkrijk

3.4.1 Europese Unie

Aanleiding
Anders dan de Verenigde Staten heeft de EU wel een overkoepelende privacy wet voor alle organisaties en sectoren, waarin een meldplicht kan worden opgenomen. Op dit moment hanteert Europa net als de Verenigde Staten een sectorale aanpak. De voorgestelde meldplicht is namelijk onderdeel van een herzieningsvoorstel van de Europese telecomwetgeving. Het Europees Parlement stemt naar verwachting voor de laatste keer over het voorstel in het voorjaar van 2009. Daarna hebben lidstaten uiterlijk 2 jaar de tijd om de meldplicht in de nationale wetgeving te implementeren. Het is niet ondenkbaar dat over een aantal jaren een meldplicht wordt ingevoerd in de overkoepelende privacy wetgeving.

Vormgeving
Binnen de Europese Unie wordt momenteel overleg gevoerd tussen het Europees Parlement, de Europese Commissie en de Raad over voorstellen voor een meldplicht binnen de Europese telecomwetgeving. Het *Europees Parlement* stelt de volgende procedure voor:
Stap 1: melding van ‘alle veiligheidsinbreuken’ aan de toezichthouder
Stap 2: in geval van *imminent and direct danger* melding aan de betrokkenen. Of melding aan betrokkenen nodig is, bepaalt de toezichthouder. De organisatie kan ook zelf besluiten meteen aan betrokkenen te melden.
Stap 3: jaarlijkse rapportage van alle veiligheidsinbreuken aan betrokkenen.
De *Europese Commissie* en de *Raad* stellen in reactie voor dat dienstaanbieders in alle gevallen *zelf* bepalen of een veiligheidsinbreuk aan de betrokkenen moet worden gemeld. Uit de reactie van enkele respondenten blijkt verder dat er nog geen eenduidigheid bestaat over de betekenis die de Europese Commissie en het Europees Parlement aan de formulering ‘alle veiligheidsinbreuken’ hechten.

In Europa is de *doelgroep* van de meldplicht als gevolg van de sectorale aanpak van de EU een belangrijk punt van discussie. Omdat de meldplicht wordt opgenomen in Europese telecomwetgeving, wordt deze alleen van toepassing op de bedrijven die binnen de reikwijdte van deze wet vallen. Momenteel verschillen de Europese Commissie en de Telecomraad enerzijds en het Europees Parlement anderzijds hierover van mening. De Europese Commissie en de Telecomraad beperken de meldplicht tot de organisaties die nu vallen onder de Europese telecomwetgeving, ofwel telecombedrijven en internet service providers (ISP's). Het Europees Parlement heeft de voorkeur voor een meldplicht die verder gaat en voor *alle* diensten van de informatiemaatschappij geldt. In dat geval zouden bijvoorbeeld ook internetbankieren, Facebook en Hyves en online zorgaanbieders onder de meldplicht vallen.

Handhaving
Een consequentie van de voorgestelde procedure is de uitbreiding van het takenpakket en bevoegdheden van de nationale toezichthouders in de lidstaten. Een belangrijke vraag is of toezichthouders voldoende capaciteit hebben om deze taken goed uit te kunnen voeren. Respondenten in Europa brengen een mogelijk tekort aan financiële en personele capaciteit als aandachtspunt naar voren.

3.4.2 Duitsland

Aanleiding
In Duitsland is de discussie over de invoering van een meldplicht vergevorderd en lijkt een meldplicht op handen. Een groot dataschandaal bij T-Mobile heeft de discussie aangewakkerd en mogelijk de invoering van een meldplicht versneld. Een wetsontwerp voor de meldplicht ligt momenteel bij het Duitse kabinet. De bedoeling is dat de wet nog voor de parlementsverkiezingen van 2009 door de Bondsdag wordt aangenomen. Onzeker is of deze termijn wordt gehaald. Als het voorstel wordt aangenomen, heeft Duitsland als tweede land in Europa een meldplicht.

Vormgeving
De voorgestelde meldplicht heeft een bredere reikwijdte dan het voorstel van de EU. Federale overheden, de overheden van de Länder en private data controllers (alle ondernemingen die persoonsgegevens verzamelen, beheren of verwerken) zouden melding moeten maken aan de toezichthouder en betrokken burgers van 'ernstige veiligheidsinbreuken'. Dit houdt in dat 'besondere' persoonsgegevens onrechtmatig zijn verspreid of op onrechtmatige wijze bekend zijn geworden bij derden en er mogelijk sprake is van ernstige schade voor betrokken burgers.

Handhaving
De data beschermingsautoriteiten worden verantwoordelijk voor de handhaving van de meldplicht. Op dit moment bevat het voorstel een boete op niet-melding; het is mogelijk dat dit nog verandert.
Duitsland voert de meldplicht mogelijk tegelijk in met een systeem van vrijwillige audits en een keurmerk. De overheid verwacht dat organisaties door de invoering van beveiligingsaudits gaan concurreren op het gebied van de bescherming van privacy.

3.4.3 Verenigd Koninkrijk

Aanleiding
In het Verenigd Koninkrijk is veel discussie onder de bevolking door de vele dataschandalen waarmee het land recentelijk is geconfronteerd. Van een in te voeren meldplicht is op dit moment echter geen sprake. De toezichthouder pleit voor een heldere afbakening van hoe, in welke gevallen en wat te melden. Het huidige voorstel op Europees niveau vindt de toezichthouder echter 'too prescriptive and too burdensome', met name voor bedrijven[1].

Sinds mei 2008 is de Information Commissioner, net als de Financial Services Authority, bevoegd om bedrijven en organisaties een boete op te leggen indien zij de Data Protection Act (DPA) schenden. Ook een veiligheidsinbreuk of gegevensverlies kunnen zo leiden tot een boete. De DPA geldt voor alle *data controllers,* ofwel alle personen en organisaties die persoonsgegevens voor een bepaald doel be-, verwerken en of beheren. Een boete kan niet direct worden opgelegd; hier gaat een procedure aan vooraf. Hoewel in het Verenigd Koninkrijk organisaties niet verplicht zijn om veiligheidsinbreuken aan de Privacy Commissioner te melden, wordt er in de praktijk wel gemeld.

De toezichthouder is van mening dat bedrijven niet gevoelig zijn voor boetes. Volgens de respondent is de boete als gevolg van schending van de DPA relatief laag; bedrijven zijn vooral gevoelig voor de imagoschade. De toezichthouder publiceert de stappen die hij tegen organisaties onderneemt dan ook op zijn website.

[1] Ron Condon, Information Commissioner turns up the heat on data breach culprits (SearchSecurity.co.uk, 30 oktober 2008)

4 Resultaten quick scan

In dit hoofdstuk zetten we de belangrijkste bevindingen van het onderzoek op een rij. In paragraaf 4.1 bespreken we de doelstellingen die ten grondslag liggen aan de invoering van een meldplicht. Vervolgens onderscheiden we in paragraaf 4.2 de elementen waardoor meldsystemen van elkaar kunnen verschillen. Paragraaf 4.3 beschrijft de argumenten die een rol spelen in discussies over invoering van een meldplicht. Vervolgens zetten we op basis van de in paragraaf 4.2 onderscheiden elementen de belangrijkste uitkomsten van de quick scan uiteen. In paragraaf 4.5 worden de bevindingen samengevat in een model.

4.1 De meldplicht in theorie

Uit het onderzoek komt naar voren dat aan de invoering van een meldplicht doorgaans de volgende hoofddoelstelling ten grondslag ligt:

Het voorkomen van schade voor burgers door veiligheidsinbreuken bij organisaties die over privacygevoelige informatie van burgers beschikken.

De vraag is dan hoe een meldplicht bijdraagt aan de realisatie van deze doelstelling. Uit het onderzoek komt naar voren dat de relatie tussen een meldplicht enerzijds en het te bereiken doel (het voorkomen van schade voor de burger door verlies van gegevens door organisaties) anderzijds, in theorie verloopt via drie sporen (zie ook figuur 4.1).

Het eerste spoor loopt via de gegevensbeherende organisaties. Uit het vorige hoofdstuk kwam naar voren dat, althans in de Verenigde Staten, slechte beveiliging van gegevenssystemen in belangrijke mate bijdraagt aan gegevensverlies. De veronderstelde werking van een meldplicht is dat deze bedrijven aanspoort de beveiliging van gegevens van burgers te optimaliseren. Dit, omdat ze al naar gelang de wijze waarop de meldplicht is vormgegeven willen voorkomen dat:

- ze een slechte naam krijgen als gevolg van de melding (bijvoorbeeld door publicatie in de media of door ‘naming & shaming’ door de toezichthouder)
- ze kosten moeten maken verbonden aan een melding (bijvoorbeeld het moeten inlichten van mogelijk grote aantallen belanghebbenden)
- toezichthouders zich actief met hen gaan bemoeien
- ze worden geconfronteerd met eventuele rechtszaken en/of strafmaatregelen.

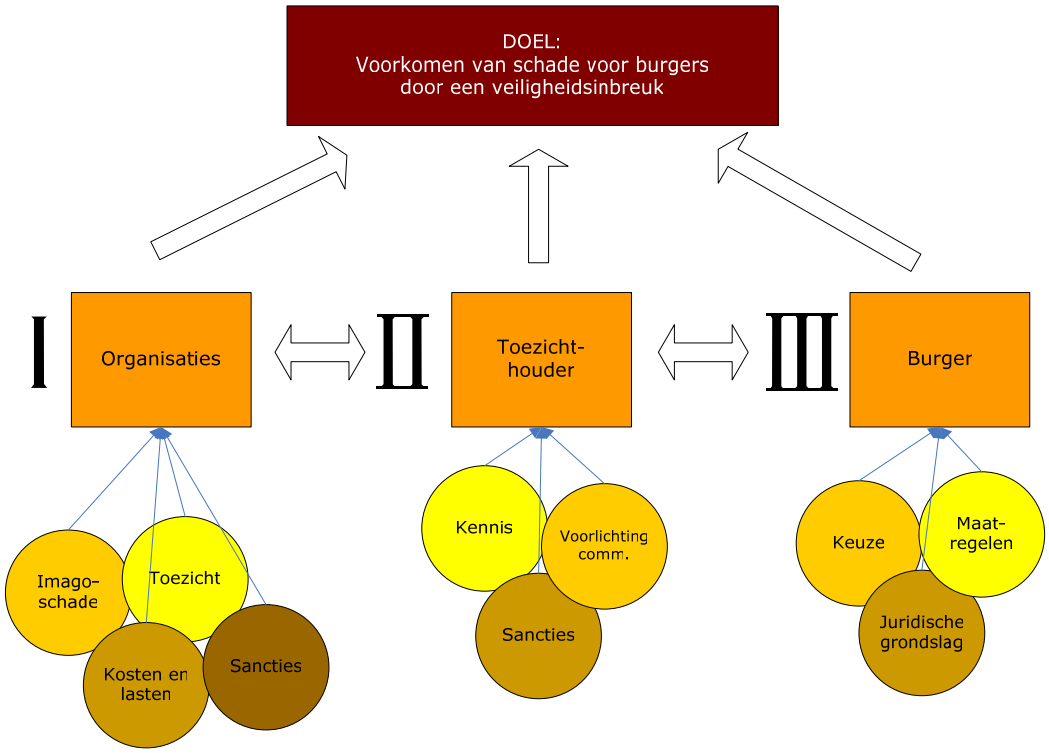
Het tweede spoor loopt via de handhaving door de overheid. Door een meldplicht zou de overheid beter inzicht krijgen in de aard en risico’s van veiligheidslekken waardoor zowel het ‘zachte’ (voorlichting, advisering) als harde toezicht (sancties) kan worden versterkt.

Het derde en laatste spoor tenslotte, loopt via de burger. De aan dit spoor ten grondslag liggende veronderstellingen zijn, afhankelijk van de vormgeving van de meldplicht, de volgende:

- door openbaarmaking van veiligheidsinbreuken, heeft de burger de mogelijkheid organisaties te beoordelen op de zorgvuldigheid van hun gegevensbeheer en kan hij op grond van deze beoordeling eventueel besluiten met een andere leverancier in zee te gaan;

- doordat organisaties burgers melden dat gegevens verloren zijn gegaan, zijn burgers mogelijk in staat tijdig maatregelen te nemen om daadwerkelijke schade te voorkomen (bijvoorbeeld het blokkeren van pinpassen);
- de meldplicht geeft burgers een juridische grondslag schade als gevolg van gegevensverlies op de betreffende organisatie te verhalen.

Figuur 4.1 De meldplicht in theorie



4.2 Elementen van meldingen

Meldsystemen verschillen van elkaar doordat ze uit verschillende elementen bestaan en/of vergelijkbare elementen bevatten die op verschillende wijze zijn geoperationaliseerd. Hieronder staan we kort stil bij de elementen die in een meldsysteem kunnen zijn opgenomen.

1 **Het doel van de melding**. In de vorige paragraaf is ingegaan op de verschillende manieren waarop de meldplicht kan werken. Voor het vormgeven van een meldsysteem is het van belang welk doel of welke doelen de melding dient: het aansporen van bedrijven hun beveiliging te optimaliseren, het versterken van de handhaving en/of het versterken van de positie van de burger.

2 **Vrijwillig of verplichte melding.** Doorgaans verplicht het meldsysteem organisaties wettelijk veiligheidsinbreuken te melden. Het onderzoek omvat echter ook systemen van vrijwillige melding.

3 **Doelgroep.** Meldsystemen kunnen zich richten op verschillende doelgroepen. Ze kunnen zijn beperkt tot bepaalde sectoren (bijvoorbeeld bedrijven en/of overheid) en/of bepaalde typen bedrijven.

4 **Soort gegevens.** Zoals eerder is aangegeven gaat het om 'persoonsgegevens'. Het is echter mogelijk dat een meldsysteem niet op alle denkbare type persoonsgegevens betrekking heeft (bijvoorbeeld het al dan niet opgenomen zijn van medische gegevens). Meldsystemen kunnen verder verschillen naar de wijze waarop gegevens zijn beveiligd. Zo zijn er meldsystemen die niet van toepassing zijn op versleutelde (encrypted) gegevens. Een ander verschil kan er in zijn gelegen dat meldingsystemen zich beperken tot elektronische (computerized) data of ook betrekking hebben op audiovisueel en/of papier vastgelegde gegevens.

5 **Grondslag voor melding: wanneer melden?** Eén van de belangrijkste en lastigst te bepalen elementen van een meldsysteem is de grondslag voor de melding, in de Verenigde Staten vaak aangeduid als de trigger. Wanneer precies moet een organisatie melding maken van gegevensverlies? Mogelijke grondslagen zijn:

- melding van *alle* veiligheidsinbreuken (zonder dat is aangetoond dat een onbevoegde daadwerkelijk gegevens heeft verkregen)
- onbevoegde *toegang* tot persoonsgegevens (idem)
- persoonsgegevens *verkregen* door onbevoegde
- risico op *misbruik* of onrechtmatige *verspreiding* van persoonsgegevens
- risico op *schade* voor betrokkenen
- a*antal* verloren gegevens of gedupeerden.

6 **Aan wie melden?** Sommige meldsystemen beperken zich tot melding aan alleen de getroffen burgers of aan alleen de overheid (bijvoorbeeld toezichthouder, Justitie). Andere omvatten melding aan beide.

7 **Handhaving en toezicht.** Meldsystemen kunnen verschillen naar de wijze waarop de handhaving en het toezicht is geregeld: is er actieve handhaving, is er een toezichthouder die handhaaft, waaruit bestaat handhaving, welke bevoegdheden heeft de handhavende instantie (bijvoorbeeld controle- en/of boetebevoegdheid, of slechts meldpunt)?

8 **Wettelijke verankering.** Moet een meldsysteem worden opgenomen in een nieuwe of worden ondergebracht in een bestaande wet? Voor Nederland is het bijvoorbeeld de vraag of een eventuele meldplicht moet worden opgenomen in de Wet Bescherming Persoonsgegevens, de Telecommunicatiewet, de Wet Economische Delicten of het Wetboek van Strafrecht.

4.3 Discussie: argumenten voor en tegen

Door de bezorgdheid over veiligheidsinbreuken en identiteitsfraude heeft de invoering van een meldplicht in de meeste onderzochte landen brede steun gekregen. Gebezigde argumenten van verschillende stakeholders voor én tegen een meldplicht zijn opgenomen in tabel 4.1.

Tabel 4.1 Argumenten voor en tegen invoering meldplicht

Voor	Tegen
Burgers hebben er recht op te weten dat hun persoonsgegevens gevaar lopen; Als burgers op de hoogte zijn van een veiligheidsinbreuk, kunnen zij tijdig maatregelen treffen om schade te voorkomen; Burgers herwinnen het vertrouwen in organisaties als deze inbreuken melden en burgers op de hoogte stellen van de maatregelen die de organisatie neemt om schade en toekomstige inbreuken te voorkomen; Een meldplicht is een stimulans voor bedrijven om meer aandacht aan de beveiliging van persoonsgegevens te schenken en deze te verbeteren om zo de imagoschade, administratieve lasten, kosten en sancties te voorkomen die met een melding gepaard gaan; Door melding te verplichten komen overheden en organisaties meer te weten over aantallen en de aard van data breaches, zodat: - de overheid de regulering kan verbeteren; - toezichthouders bedrijven en organisaties beter kunnen begeleiden bij het omgaan met veiligheidsinbreuken en het verbeteren van de beveiliging; - organisaties hun beveiliging kunnen verbeteren.	(Overvloedige) melding van veiligheidsinbreuken maakt burgers: - angstig en nodeloos ongerust, want slechts een klein deel van alle veiligheidsinbreuken leidt tot identiteitsfraude; - onverschillig voor meldingen en niet meer bereid te reageren op de serieuze gevallen; Uit angst voor imagoschade na melding van een veiligheidsinbreuk, zullen organisaties deze juist intern willen houden; De procedure van melding brengt hoge kosten en administratieve lasten voor bedrijven met zich mee; De private sector heeft de beveiliging al goed op orde: een meldplicht is niet nodig; Preventie en verbetering van veiligheidsmaatregelen verdienen de voorkeur boven een meldplicht; Een meldplicht levert problemen op met aansprakelijkheid; omdat het vaak onduidelijk is wie de dader is en hoe en waar een veiligheidsinbreuk heeft plaatsgevonden, is het niet duidelijk wie voor de kosten van een melding moet opdraaien; De financiële crisis heeft het vertrouwen in banken van de consument al geschaad; door banken te verplichten veiligheidsinbreuken te melden, neemt dit vertrouwen nog verder af.

4.4 Bevindingen

In deze paragraaf beschrijven we de bevindingen voor elk van de in paragraaf 4.2 onderscheiden elementen van een meldsysteem. We beginnen met de doelstellingen van onderzochte meldsystemen.

4.4.1 Doel van de melding

In geen van de in het onderzoek betrokken landen waren voor de invoering van een meldsysteem dan wel de discussie over de invoering daarvan betrouwbare gegevens bekend over gegevensverlies en de gevolgen daarvan. Een belangrijk motief om een meldsysteem in te voeren dan wel de discussie daarover te starten zijn incidenten waarbij gegevens zijn verloren en het toenemende aantal klachten van burgers over misbruik van hun persoonsgegevens. Dataschandalen in de Verenigde Staten en het Verenigd Koninkrijk liggen mede ten grondslag aan het besluit van Australië en Canada een meldsysteem in te voeren.

Verenigde Staten
In de Verenigde Staten heeft de meldplicht in de eerste plaats ten doel bedrijven aan te zetten de beveiliging van hun databases te optimaliseren, teneinde imagoschade als gevolg van het moeten melden van gegevensverlies te voorkomen. In de tweede plaats moet de meldplicht burgers in staat stellen maatregelen te nemen tegen verlies van hun gegevens, bijvoorbeeld het tijdig blokkeren van creditcards.

In tegenstelling tot het Nederlandse burger servicenummer (BSN), kan het vergelijkbare Amerikaanse social security number (SSN) ook voor commerciële doeleinden worden gebruikt. Hierdoor zijn Amerikaanse burgers vatbaarder voor schade bij verlies van het nummer. In een aantal gevallen heeft de meldplicht tevens ten doel burgers een juridische grond te verschaffen voor gerechtelijke procedures tegen bedrijven die hun gegevens hebben verloren.

Het doel van de meldplicht om het burgers mogelijk te maken tegen organisaties die hun gegevens zijn kwijtgeraakt te procederen hangt samen met het Amerikaanse rechtssysteem. In de eerste plaats kennen de Verenigde Staten geen overkoepelende privacy-wetgeving waarin de bescherming van persoonsgegevens is vastgelegd zoals in vele Europese landen, waaronder Nederland, wel het geval is. In de tweede plaats is het Amerikaanse rechtsysteem er in vergelijking tot onder meer het Nederlandse systeem meer op gericht om via juridische procedures achteraf geleden schade op de veroorzaker te verhalen. In het Nederlandse systeem speelt preventie, het voorkomen van schade, door zelfregulering en/of toezicht en handhaving een belangrijke rol.

Andere landen
Uit een onderzoek waarvoor in ‘privacy commissioners’ in Europa zijn benaderd blijkt dat zij het erover eens zijn dat (enige vorm van) meldplicht nuttig zou zijn[1]. Denemarken, Tsjechië, Hongarije, Frankrijk, IJsland, Spanje en Zwitserland zijn van mening dat de bestaande

1 Stewart Dresner, Chief Executive, Privacy Laws & Business, presentatie tijdens THE PRIVACY SYMPOSIUM - SUMMER 2008, HARVARD: PRIVACY IN TRANSITION (August 18th – 21st 2008) getiteld The prospects of data breach laws in 18 European countries. Het onderzoek bevat meningen van toezichthouders in de volgende landen: Tsjechische Republiek, Denemarken, Finland, Guernsey, Hongarije, IJsland, Ierland, Jersey, Slowakije, Zweden, Verenigd Koninkrijk, Italië, Spanje, Portugal, Polen, Luxemburg, Frankrijk en België.

privacy wetgeving voldoende is om met gegevensverlies om te gaan. Slowakije, België en Ierland hebben hierover geen uitgesproken mening.[1]

Uit het citaat in paragraaf 1.1 over de doelstelling van het opnemen van een meldplicht in de Europese telecommunicatierichtlijn is duidelijk dat het doel hiervan is dat bedrijven, mede door versterking van toezicht en handhaving, hun veiligheidssystemen verbeteren. Ook in andere door ons onderzochte landen is de stimulans die van een meldsysteem uitgaat voor bedrijven om hun systemen optimaal te beveiligen een belangrijke argument voor invoering van een dergelijk systeem.

In Noorwegen, Canada en Australië heeft het systeem ook duidelijk ten doel de toezichthouder beter te informeren over de mate waarin veiligheidsinbreuken voorkomen en de aard van deze inbreuken. Deze kennis moet de toezichthouder in staat stellen bedrijven beter te kunnen voorlichten en adviseren over hoe veiligheidsinbreuken te voorkomen.
In Duitsland wil de overheid bedrijven stimuleren veiligheidsinbreuken te melden om te voorkomen dat deze pas lang na dato via de pers bekend worden (zoals het geval was bij T-mobile).

4.4.2 Verplichte of vrijwillige melding

Doorgaans is de melding verplicht of gaan de gedachten uit naar een verplichte melding. Een uitzondering hierop vormen momenteel Australië, Nieuw-Zeeland en Canada. In Australië is de melding (vooralsnog) vrijwillig omdat de overheid in nauwe samenwerking met het bedrijfsleven wil komen tot een meldplicht die draagvlak heeft onder het bedrijfsleven. Omdat vrijwillige melding te weinig informatie over veiligheidsinbreuken oplevert, overweegt Canada ook een meldplicht in te voeren.

4.4.3 Doelgroep

Wat betreft de doelgroep van een meldsysteem is een aantal keuzemogelijkheden voorhanden (zie figuur 4.2).

Figuur 4.2 Doelgroepen

[1] Idem

In de keuzes die zijn gemaakt blijkt een scheidslijn zichtbaar tussen enerzijds de federale overheid van de Verenigde Staten en de Europese Unie en anderzijds de Amerikaanse deelstaten en de nationale overheden van andere landen.

Amerikaanse deelstaten en nationale overheden: brede reikwijdte
De meeste Amerikaanse deelstaten en nationale overheden buiten de Verenigde Staten hebben gekozen voor een meldplicht voor alle organisaties die binnen de grenzen van de staat of het land *werkzaam* zijn[1]. Hierbij wordt geen onderscheid gemaakt tussen het bedrijfsleven en (semi-)overheid[2].

Een aantal toezichthouders in Europa geeft de voorkeur aan een meldplicht die voor zowel de private als de publieke sector geldt. Europese toezichthouders vinden daarnaast dat zowel data processors als controllers eronder moeten vallen[3].

Federale overheid Verenigde Staten en Europese Unie: doelgroepen beperkt
Door de afwezigheid van overkoepelende privacy wetgeving voor alle organisaties en de sectorale aanpak, is op federaal niveau in de Verenigde Staten alleen voor een aantal sectoren en organisaties een meldplicht van toepassing.

Binnen de Europese Unie is de doelgroep van de meldplicht een belangrijk punt van discussie. Omdat de meldplicht wordt opgenomen in Europese telecomwetgeving, zou deze alleen van toepassing zijn op de bedrijven die binnen de reikwijdte van deze wet vallen. Momenteel verschillen enerzijds de Europese Commissie en de Telecomraad en anderzijds het Europees Parlement hierover van mening. De EC en de Raad willen de meldplicht beperken tot de telecomsector; het Parlement heeft de voorkeur voor een meldplicht die verder gaat en voor *alle* diensten van de informatiemaatschappij geldt.

Het is nog de vraag of de lidstaten in Europa de sectorale aanpak van de EU zullen overnemen of dat zij zich op meerdere doelgroepen zullen richten. Hierbij speelt een aantal overwegingen een rol:
- Willen lidstaten verder gaan dan de Europese meldplicht? Wat is de doelgroep van de meldplicht? Moet de meldplicht gelden voor alleen de private of ook de publieke sector?
- Rol en capaciteit toezichthouders: hoe een meldplicht handhaven als deze een zeer brede reikwijdte heeft?

[1] Overzichten meldplichten in Amerikaanse deelstaten door Attorney Julie Brill uit de staat Vermont (Comparison of Security Breach Laws updated 7/12/07) en de Consumer's Union (Notice of Security Breach State Laws, Last updated August 21, 2007)

[2] In enkele deelstaten in de Verenigde Staten is de doelgroep beperkter dan data controllers. In sommige staten geldt de meldplicht voor alle organisaties die persoonsgegevens a) verzamelen (data collector) b) ver- of bewerken (data processor) c) beheren (data controller) e) onderzoeken (data broker). Data brokers zijn organisaties die in opdracht databases met (persoons-) informatie doorzoeken, bijvoorbeeld onderzoeksbureaus. Afgeleid van Dr. Demi Getschko, Malcolm Harbour, Henry L. Judy, David Satola, Rajnesh Singh, presentatie tijdens Internet Governance Forum (Rio de Janeiro Brazil, November 2007) getiteld: Global Best Practices - Consumer Protection and Data Breach Notification.

[3] Data collectors zijn organisaties die persoonsgegevens verzamelen; data processors ver- of bewerken persoonsgegevens. Stewart Dresner, Chief Executive, Privacy Laws & Business, *The prospects of data breach laws in 18 European countries.* Het onderzoek bevat meningen van toezichthouders in de volgende landen: Tsjechische Republiek, Denemarken, Finland, Guernsey, Hongarije, IJsland, Ierland, Jersey, Slowakije, Zweden, Verenigd Koninkrijk, Italië, Spanje, Portugal, Polen, Luxemburg, Frankrijk en België.

Alleen privaat
In enkele deelstaten in de Verenigde Staten geldt de meldplicht alleen voor de private sector.

4.4.4 Soort gegevens

Het gaat bij een meldplicht altijd om persoonsgegevens. Hierbinnen wordt onderscheid gemaakt tussen de kenmerken inhoud, gegevensdrager en mate van beveiliging (zie figuur 4.3).

Figuur 4.3 Soort gegevens

Inhoud
In de Verenigde Staten wordt gewoonlijk de volgende definitie van de term 'persoonsgegevens' gehanteerd:

'An individual's first name or first initial and last name, in combination with any one or more of national ID number, drivers license number, medical information or financial account number, combined with any required security or access code or password that would permit access to an individual's financial account'[1].

Een trend in de Verenigde Staten is om medische gegevens onder de meldplicht te laten vallen. De federale wet die voor de gezondheidszorg geldt, HIPAA, is namelijk niet expliciet over veiligheidsinbreuken van medische gegevens.

In een aantal landen, waaronder Australië, Duitsland en Noorwegen, geldt de meldplicht voor 'gevoelige' gegevens. Hieronder worden persoonsgegevens verstaan gerelateerd aan:
- een ambtsgeheim;
- etnische origine;
- politieke, filosofische of religieuze overtuigingen;
- het feit dat een persoon is verdacht van een misdrijf of daarvoor is aangeklaagd of veroordeeld;
- gezondheid;
- seksuele voorkeur;
- lidmaatschap van een vakbond[2].

[1] Dr. Demi Getschko, Malcolm Harbour, Henry L. Judy, David Satola, Rajnesh Singh, Global *Best Practices - Consumer Protection and Data Breach Notification* en overzicht van Attorney Julie Brill. Veel Amerikaanse deelstaten maken een uitzondering voor openbare informatie waarvan het wettelijk is toegestaan dat zij openbaar zijn gemaakt. Hiermee worden gegevens bedoeld uit openbare overheidsdatabases of media.
[2] Personal Data Act: Act of 14 april 2000 No. 31 relating to the processing of personal data, Chapter I, Section 2, 8 a t/m e

Gegevensdrager
De meldplicht kan worden afgebakend met behulp van de drager waarop de persoonsgegevens zijn opgeslagen. In de meeste landen is de meldplicht alleen van toepassing op *computerized* gegevens. Gewoonlijk worden onder 'computerized' digitale gegevens verstaan; gegevens die zijn opgeslagen op de computer, laptop of memorystick. In Australië is men van mening dat de meldplicht zo breed mogelijk moet zijn en niet beperkt tot digitale gegevens. Hoewel papieren data in de Verenigde Staten in principe niet onder de meldplicht vallen, worden inbreuken van papieren data in de praktijk *wel* gemeld, blijkt uit de casestudy Californië.

Mate van beveiliging
Bijna zonder uitzondering kiezen deelstaten in de Verenigde Staten ervoor versleutelde gegevens uit te sluiten van de meldplicht (encryptie). Er wordt ten eerste vanuit gegaan dat het risico op schade kleiner is als de gegevens zijn versleuteld. Daarnaast is dit een van de manieren waarop overheden organisaties proberen te stimuleren meer aandacht aan beveiliging te schenken, met name aan de beveiliging van *carry on media*. Na invoering van de meldplicht in Californië bleek namelijk dat veel inbreuken het gevolg waren van gestolen laptops en memoriesticks met informatie die niet was beveiligd.

Andere landen zijn kritischer over het uitsluiten van versleutelde persoonsgegevens als onderdeel van de meldplicht. Ook een aantal Nederlandse respondenten stelt zich kritisch op: deencryptie is immers altijd mogelijk. Aan de andere kant zien Nederlandse respondenten wel wat in het argument dat eisen aan encryptie bedrijven stimuleert om hun data beter te beveiligen.

4.4.5 Grondslag voor melding

De grondslag moet voorkomen dat burgers en toezichthouders overspoeld worden met meldingen. Ook kan een heldere afbakening van te melden incidenten administratieve lasten en kosten voor bedrijven beperken. Het bepalen van deze grondslag voor melding blijkt een van de meest lastige beslissingen. Onenigheid over de grondslag is volgens respondenten bijvoorbeeld de hoofdreden dat het Amerikaanse Congres nog niet gekomen is tot een overkoepelende meldplicht. Uit het onderzoek kwam een aantal mogelijke grondslagen naar voren (zie figuur 4.4).

Figuur 4.4 Grondslagen

Meestal verkrijgen van persoonsgegevens of schade
In de Verenigde Staten en daarbuiten is de grondslag meestal het verkrijgen van persoonsgegevens (acquisition of data) en een risico op (een vorm) van schade voor de betrokkenen. Onder 'schade' wordt in de Verenigde Staten meestal financiële schade verstaan. In andere landen schaart men er ook imagoschade en andere vormen van schade in relatie tot de persoonlijke levenssfeer onder.

Enkele deelstaten en landen vereisen reeds melding wanneer er een veiligheidsinbreuk heeft plaatsgevonden, zonder dat hoeft te worden aangetoond dat toegang is verkregen tot persoonsgegevens. De meeste landen geven hier niet de voorkeur aan, omdat dit veel meldingen op zou kunnen leveren en zo nodeloos angst kan inboezemen bij consumenten. Het aantal verloren gegevens of gedupeerden wordt vrijwel nooit als grondslag gebruikt; het verlies van creditcardgegevens kan voor één persoon immers al erg schadelijk zijn.

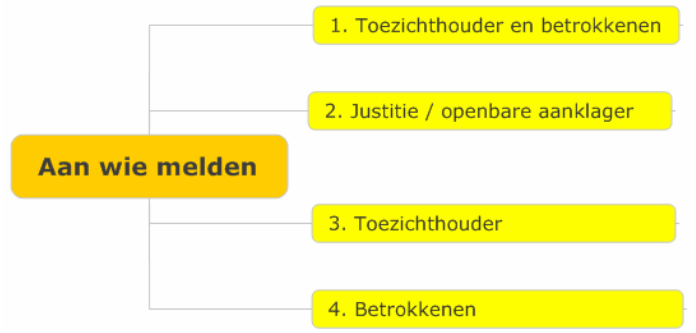
Europa: nog niet uitgekristalliseerd
In Europa zijn de meningen en ideeën over de grondslag nog niet uitgekristalliseerd. Binnen de Europese Unie wordt momenteel voorgesteld de volgende grondslag te hanteren: melding van 'alle veiligheidsinbreuken' aan de toezichthouder, en in geval van *imminent and direct danger*, melding aan de betrokkenen. Uit de reactie van enkele respondenten blijkt dat er nog geen eenduidigheid bestaat over de betekenis die de Commissie en het Parlement aan de grondslag 'alle veiligheidsinbreuken' hechten. Volgens een respondent bedoelt de Commissie hiermee alleen ernstige inbreuken. Een andere respondent stelde dat het Parlement dit letterlijk interpreteert als *alle* veiligheidsinbreuken.

4.4.6 Aan wie melden?

De meldplicht vereist in alle landen in ieder geval melding aan de getroffen personen wier persoonsgegevens gevaar lopen als gevolg van een veiligheidsinbreuk. Het is ook mogelijk dat een organisatie een veiligheidsinbreuk eerst moet melden aan een toezichthouder of justitie (openbare aanklager). In een aantal landen wordt dan samen bepaald of melding

aan burgers nodig is. Dit is het geval in een aantal Amerikaanse deelstaten. Ook in de Australische voorstellen voor een meldplicht wordt een soortgelijke procedure toegepast.

Figuur 4.5 Aan wie melden?



Vorm en inhoud van de melding

De meldplicht schrijft vrijwel altijd voor dat de melding op het meest gunstige moment en zonder uitstel aan de betrokkenen wordt gemeld. De meeste overheden stellen eisen aan de vorm en inhoud van een melding. In de Verenigde Staten zijn deze eisen tot in detail uitgewerkt. Hier moeten organisaties de getroffenen meestal schriftelijk op de hoogte stellen, omdat een e-mail onvoldoende vertrouwen wekt. In Australië is de vorm van de melding vrij.

Respondenten in zowel de Verenigde Staten als Europa, Australië en Nederland hechten veel waarde aan de inhoud van de melding. Zij vinden het belangrijk dat de melding in ieder geval advies en een follow-up bevat over maatregelen die de consument kan nemen om schade te voorkomen. In de Verenigde Staten en Australië is dit het verst uitgewerkt[1]. Binnen de Europese Unie en de lidstaten verkeren ideeën over de inhoud van deze follow-up nog in een verkennend stadium.

4.4.7 Handhaving en toezicht

Wie handhaaft?

In de Verenigde Staten is de District Attorney vaak verantwoordelijk voor handhaving van de meldplicht; in andere landen is dit de nationale toezichthouder.

Verenigde Staten: District Attorney

In de Verenigde Staten vindt in principe geen actieve handhaving plaats. Dit land kent geen centrale toezichthouder die privacy wetgeving handhaaft, zoals de landen in Europa en Canada en Australië. In de meeste Amerikaanse deelstaten moeten organisaties inbreuken dan ook alleen aan de getroffen burgers melden. Als een deelstaat ervoor kiest om de meldplicht te handhaven, komt dit neer op de District Attorney, die verantwoordelijk is voor de bescherming van de privacy van burgers.

[1] Voor voorbeelden van voorgeschreven vormen van meldingen in de Verenigde Staten zie *Security breaches chart* van Julie Brill. Voor Australië, zie *Guide to handling personal information security breaches*, opgesteld door Office of the Privacy Commissioner.

Andere landen: toezichthouder

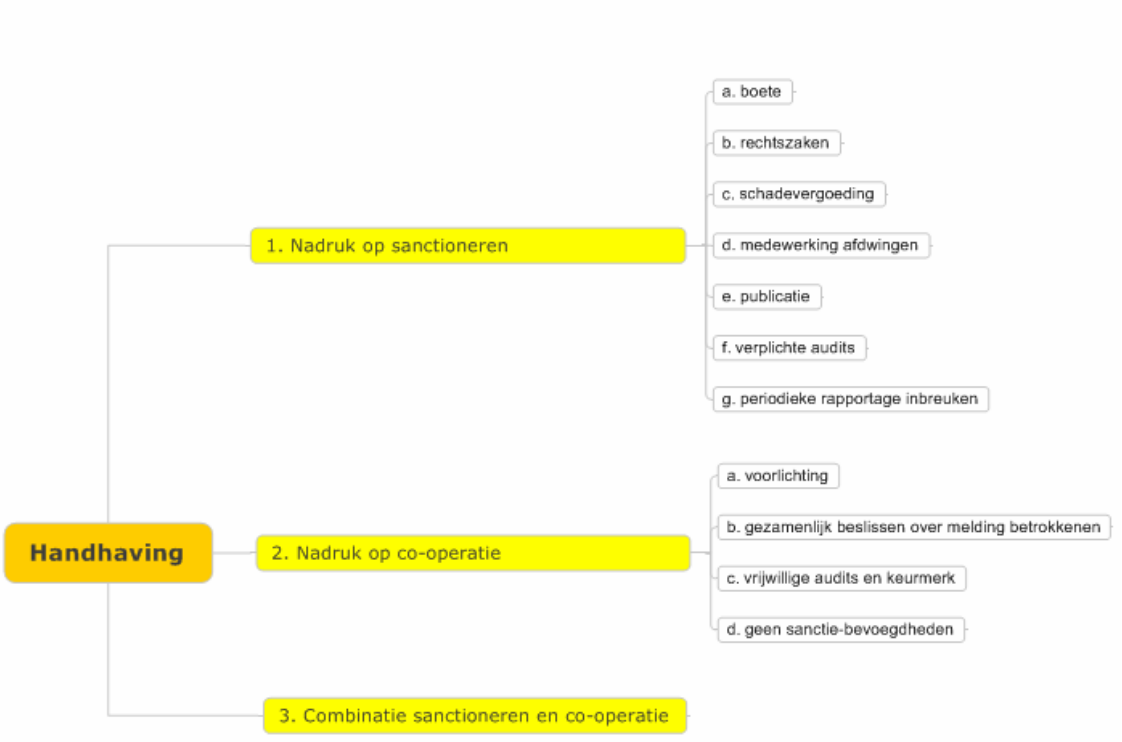
In andere landen met vrijwillige of verplichte melding (Canada, Australië, Noorwegen) kiest men vrijwel altijd naast melding aan het individu voor melding aan de toezichthouder. Landen die overwegen een meldplicht in te voeren en geïnterviewde experts in Nederland geven hier ook de voorkeur aan. Een groot aantal toezichthouders in Europese lidstaten vindt dat organisaties hen op de hoogte zouden moeten stellen van veiligheidsinbreuken[1]. Door melding aan een toezichthouder krijgt deze:

- de kans om samen met de organisatie te bepalen of melding nodig is;
- meer kennis van aantallen en aard van veiligheidsinbreuken, waardoor hij organisaties beter kan adviseren over beveiliging van systemen en het omgaan met veiligheidsinbreuken.

Hoe handhaven?

Een aantal landen legt meer nadruk op handhaving door sanctionering, terwijl andere landen de voorkeur geven aan handhaving door co-operatie en communicatie. Andere landen bevinden zich tussen beide vormen in (zie figuur 4.6).

Figuur 4.6 Handhaving



Nadruk op sanctioneren

De Verenigde Staten legt de nadruk op sanctionering achteraf. Op niet melden staat in een groot aantal Amerikaanse staten een boete. Wanneer de District Attorney verantwoordelijk is voor de handhaving van de meldplicht, mag hij daartoe rechtszaken aanspannen, mede-

[1] Naast het Verenigd Koninkrijk ook Guernsey, Tsjechië, Ierland, Finland, Frankrijk, Portugal, Luxemburg, Italië. Stewart Dresner, Chief Executive, Privacy Laws & Business, *The prospects of data breach laws in 18 European countries*

werking van bedrijven afdwingen en een schadevergoeding eisen. Omdat organisaties zich naar verwachting niet altijd aan de meldplicht houden, hechten ook geïnterviewde Nederlandse experts veel belang aan toezicht en handhaving door sanctioneren.

Ook in de voorstellen van de Europese Unie ligt de nadruk op sanctionering. Organisaties worden verplicht veiligheidsinbreuken in ieder geval altijd aan de toezichthouder te melden. Providers zouden daarnaast worden verplicht tot een jaarlijkse rapportage van veiligheidsinbreuken aan de toezichthouder en de getroffen gebruikers. De Europese Unie stelt voor de rol en bevoegdheden van toezichthouders verder uit te breiden, mogelijk met een boetebevoegdheid.

Nadruk op co-operatie en communicatie
Australië en Noorwegen hebben een voorkeur voor handhaving op basis van co-operatie en communicatie. De nadruk ligt op het geven van voorlichting over het omgaan met veiligheidsinbreuken. De toezichthouders in deze landen hechten weinig waarde aan boetes. Ten eerste willen zij organisaties niet ontmoedigen veiligheidsinbreuken te melden en de toezichthouder om advies te vragen over beveiliging. Ten tweede zeggen toezichthouders dat bedrijven gevoeliger zijn voor publicatie dan boetes.

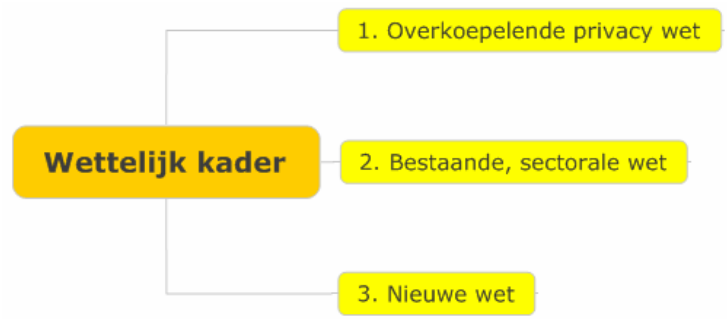
Combinatie van beide
In Duitsland wordt een combinatie van sanctioneren en co-operatie overwogen. De Duitse regering stelt voor om *vrijwillige* data beveiligingsaudits en een keurzegel voor ondernemingen in te voeren. De overheid rekent erop dat ondernemingen zelf gaan concurreren op het gebied van privacy bescherming. Het is mogelijk dat in Duitsland ook een boete komt te staan op niet-melden.

Capaciteit toezichthouders
Respondenten wijzen op het belang van voldoende financiële en personele capaciteit van toezichthouders om een (brede) meldplicht te kunnen handhaven. Met het oog op de invoering van een meldplicht, wordt binnen de Europese Unie, Canada en Australië gepleit voor een uitbreiding van de capaciteit van de toezichthouders.

4.4.8 Wettelijk kader

Uit het onderzoek komt naar voren dat de meldplicht in verschillende landen in verschillende wetgeving is opgenomen. Deze keuze is voor een deel afhankelijk van de staatsstructuur.

Figuur 4.7 Wettelijk kader



Omdat een overkoepelende privacy wet in de Verenigde Staten ontbreekt, heeft de federale overheid in de Verenigde Staten een meldplicht opgenomen in een aantal sectorale wetten. De Amerikaanse deelstaten voeren een meldplicht in overkoepelende wetgeving in of in een aparte wet. In de Verenigde Staten heeft invoering door een deelstaat vaak tot doel om de gaten op te vullen waar geen federale meldplicht geldt. De federale overheid hanteert namelijk niet alleen een sectorale aanpak, maar heeft ook (nog) niet voor alle sectoren en organisaties een meldplicht ingevoerd.

Andere landen en de Europese Unie kennen wel overkoepelende privacy wetgeving. Een aantal landen, te weten Australië, Duitsland en Noorwegen, heeft tijdens de herziening van de privacy wetgeving voorgesteld een meldplicht in te voeren. De Europese Unie stelt voor om een meldplicht op te nemen in de Europese telecomwetgeving, welke momenteel wordt herzien.

4.4.9 Bevindingen samengevat: model meldplicht

Op de volgende pagina zijn de bevindingen van de quick scan samengevat in een model. Het model brengt de submodellen uit paragraaf 4.3 bijeen en biedt zo een integraal overzicht van de keuzes die de onderzochte overheden van andere landen hebben gemaakt bij de vormgeving, invoering en handhaving van de meldplicht. Per element (doelgroep, soort gegevens, grondslag, aan wie melden, handhaving en wettelijk kader) zijn de geïnventariseerde mogelijkheden weergegeven. Per mogelijkheid geeft het model vervolgens aan welke landen ervoor hebben gekozen.

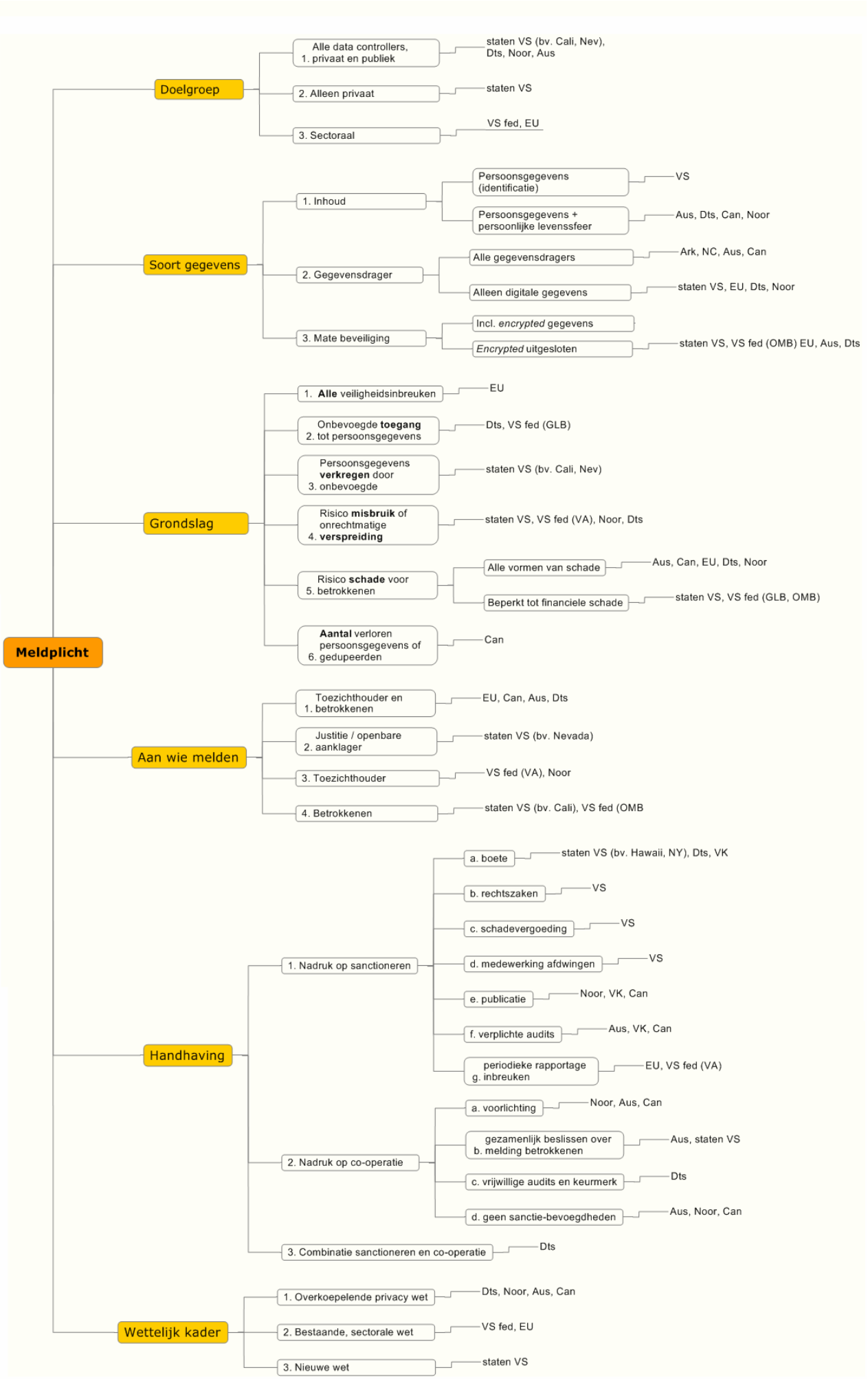
Omdat vrijwillige melding in Canada en Australië van tijdelijke aard is en zal worden vervangen door verplichte melding, is vrijwillige melding niet opgenomen.

De onderstaande legenda verklaart de afkortingen van de verschillende landen zoals gebruikt in het model.

Figuur 4.8 Bevindingen samengevat: legenda en model meldplicht

Legenda

Afkorting	***Betekenis***
Staten VS	Deelstaten in de Verenigde Staten
• Cali	• Californië
• Nev	• Nevada
• NY	• New York
• Ark	• Arkansas
• NC	• North Carolina
VS fed	Federale overheid van de Verenigde Staten
• GLB	• Gramm-Leach-Bliley Act
• OMB	• Office of Management and Budget Guidance
• VA	• Veterans' Affairs Information Security Act
EU	Europese Unie
EC	Europese Commissie
EP	Europees Parlement
ETC	Europese Telecomraad
Dts	Duitsland
VK	Verenigd Koninkrijk
Noor	Noorwegen
Can	Canada
Aus	Australië
NZ	Nieuw Zeeland


Meldplicht
Doelgroep
Alle data controllers, 1. privaat en publiek
staten VS (bv. Cali, Nev), Dts, Noor, Aus
2. Alleen privaat
staten VS
3. Sectoraal
VS fed, EU
Soort gegevens
1. Inhoud
Persoonsgegevens (identificatie)
VS
Persoonsgegevens + persoonlijke levenssfeer
Aus, Dts, Can, Noor
2. Gegevensdrager
Alle gegevensdragers
Ark, NC, Aus, Can
Alleen digitale gegevens
staten VS, EU, Dts, Noor
3. Mate beveiliging
Incl. encrypted gegevens
Encrypted uitgesloten
staten VS, VS fed (OMB) EU, Aus, Dts
Grondslag
1. Alle veiligheidsinbreuken
EU
Onbevoegde toegang 2. tot persoonsgegevens
Dts, VS fed (GLB)
Persoonsgegevens verkregen door 3. onbevoegde
staten VS (bv. Cali, Nev)
Risico misbruik of onrechtmatige 4. verspreiding
staten VS, VS fed (VA), Noor, Dts
Risico schade voor 5. betrokkenen
Alle vormen van schade
Aus, Can, EU, Dts, Noor
Beperkt tot financiele schade
staten VS, VS fed (GLB, OMB)
Aantal verloren persoonsgegevens of 6. gedupeerden
Can
Aan wie melden
Toezichthouder en 1. betrokkenen
EU, Can, Aus, Dts
Justitie / openbare 2. aanklager
staten VS (bv. Nevada)
3. Toezichthouder
VS fed (VA), Noor
4. Betrokkenen
staten VS (bv. Cali), VS fed (OMB
Handhaving
1. Nadruk op sanctioneren
a. boete
staten VS (bv. Hawaii, NY), Dts, VK
b. rechtszaken
VS
c. schadevergoeding
VS
d. medewerking afdwingen
VS
e. publicatie
Noor, VK, Can
f. verplichte audits
Aus, VK, Can
periodieke rapportage g. inbreuken
EU, VS fed (VA)
2. Nadruk op co-operatie
a. voorlichting
Noor, Aus, Can
gezamenlijk beslissen over b. melding betrokkenen
Aus, staten VS
c. vrijwillige audits en keurmerk
Dts
d. geen sanctie-bevoegdheden
Aus, Noor, Can
3. Combinatie sanctioneren en co-operatie
Dts
Wettelijk kader
1. Overkoepelende privacy wet
Dts, Noor, Aus, Can
2. Bestaande, sectorale wet
VS fed, EU
3. Nieuwe wet
staten VS

4.5 Is een meldplicht effectief? Gebrek aan empirische gegevens

Ons is een beperkt aantal evaluaties van de meldplicht bekend (zie kader). Door de recente invoering van meldsystemen biedt de literatuur onvoldoende (gefundeerd) inzicht in de effectiviteit van de Amerikaanse meldplicht. Ook onze gesprekspartners beschikken niet over harde gegevens. Er is geen empirisch bewijs dat een meldplicht bijdraagt aan het voorkomen of een afname van veiligheidsinbreuken of schade voor burgers. Ook is niet geëvalueerd hoe burgers reageren op een melding. Tot slot zijn geen gegevens bekend over de mate van naleving van de meldplicht door organisaties.

Beperkt geëvalueerd

- Volgens een recente studie van de Carnegie Mellon University heeft de invoering van een meldplicht 'a marginal effect' op de afname van identiteitsfraude en is het aantal incidenten er met 'just under 2%, on average' door gereduceerd[1].
- Een onderzoek van de Universiteit van Berkeley uit 2007, waarvoor interviews zijn gehouden met 7 *information officers* bij organisaties in de Verenigde Staten, wijst uit dat deze organisaties na invoering van de meldplicht intern meer aandacht gingen besteden aan beveiliging[2].
- Een recente studie van het Centre for Information Policy Leadership belicht een aantal elementen van de Amerikaanse meldplicht waar andere landen rekening mee zouden moeten houden bij het instellen van een meldplicht. Volgens het Centre hanteren landen buiten de VS die momenteel bezig zijn met de invoering van een meldplicht een te brede definitie van de term 'veiligheidsinbreuk'. Ook zouden zij onterecht teveel waarde hechten aan melding aan burgers om veiligheidsinbreuken en ID-fraude aan te pakken.[3]

Effecten meldplicht voor burgers?

Na invoering van een meldplicht worden burgers meer op de hoogte gesteld over veiligheidsinbreuken, denken respondenten. Volgens enkele respondenten te vaak. In de praktijk lijken voor burgers echter weinig middelen beschikbaar om zelf invloed uit te kunnen oefenen en schade te beperken. Dit geldt met name voor identiteitsfraude. Feitelijk rest de consument alleen het blokkeren van een pinpas of creditcard en het alert zijn op mutaties op de bankrekening.

Effecten meldplicht gedrag organisaties?

Een aantal respondenten denkt dat sinds de invoering van de meldplicht organisaties wel meer aandacht zijn gaan besteden aan de beveiliging van hun systemen. Een respondent leidt dit af uit stijgende uitgaven aan encryptie-software en een toenemend aantal congressen dat over dit onderwerp wordt belegd. Het is niet bekend of er een causale relatie is met de invoering van de meldplicht. Andere respondenten vermoeden daarentegen dat veel veiligheidsinbreuken na invoering van de meldplicht alsnog niet worden gemeld.

[1] Carnegie Mellon University, Do Data Breach Disclosure Laws Reduce Identity Theft? (September, 2008)
[2] Berkeley University, Security Breach Notification Laws: Views from Chief Security Officers (December 2007) Hyperlink: http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf
[3] Cate, F.H., Information Security Breaches: Looking back & thinking ahead (The Centre for Information Policy Leadership, 2008) Hyperlink: http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf

5 Vormgeving meldplicht in Nederland

Nederland kent op dit moment nog geen meldsysteem. Zoals beschreven in paragraaf 4.3 en in de casestudy over de Europese Unie in Deel II van dit rapport, neemt het Europees Parlement naar verwachting in de lente van 2009 een meldplicht aan voor de telecomsector. Vanaf dat moment hebben lidstaten uiterlijk 2 jaar de tijd om de meldplicht te implementeren in eigen wetgeving. De meldplicht op Europees niveau harmoniseert tot op zekere hoogte de implementatie van een meldplicht in de lidstaten. Op het moment van schrijven heeft de EU nog geen richtlijnen voor implementatie opgesteld. Inmiddels is er wel een politiek akkoord bereikt waarin de meldplicht is opgenomen. Hoe zou deze Europese meldplicht moeten worden vormgegeven in Nederland?

In deze paragraaf bespreken we de ontwikkeling van de discussie over de invoering van een meldplicht in Nederland en de mening van de geïnterviewde experts over de vormgeving ervan.

5.1 2005: Discussie komt op gang

Tijdens het debat over de aanpassing van de Wet Computercriminaliteit in 2005, stellen de Tweede Kamerleden Van Dam en Gerkens (PvdA en SP) per motie de invoering van een meldplicht voor.

Motie Van Dam, Gerkens

"(...) overwegende, dat burgers en bedrijven het recht moeten hebben te weten dat hun gegevens in verkeerde handen terecht zijn gekomen of kunnen zijn gekomen; verzoekt de regering een voorstel uit te werken dat leidt tot de verplichting van bedrijven, overheden en andere organisaties om burgers en bedrijven te informeren dat hun gegevens ontvreemd zijn, of dat de systemen van de organisatie gehackt zijn en hiermee voor 1 juni 2006 naar de Kamer te komen"[1].

De discussie naar aanleiding van deze motie kwam in 2005 niet verder dan argumenten voor en tegen de invoering van een meldplicht. Vragen hoe een meldplicht en de handhaving daarvan vorm te geven waren in het geheel niet aan de orde. Als argumenten voor invoering van een meldplicht droeg de oppositie aan:

- burgers en bedrijven hebben het recht te weten dat hun gegevens in verkeerde handen terecht zijn gekomen of kunnen zijn gekomen;
- na een melding kan een klant adequaat handelen;
- zelf-regulering heeft geen zin: bedrijven concurreren niet op het punt van informeren over veiligheidsinbreuken;
- een meldplicht stimuleert bedrijven om hun beveiliging op orde te hebben;
- de overheid verstrekt te weinig informatie aan burgers over de manieren waarop zij zich kunnen weren tegen criminele activiteiten en hun computer veiliger kunnen maken: 'het is een tijdelijk gat dat wij moeten dichten'.

[1] (c) 2005, VirusAlert, 'PvdA en SP klant informeren na hack' (27 september 2005)

De regeringspartijen, de toenmalige minister van Justitie en ook de Consumentenbond waren geen voorstander van het invoeren van een meldplicht. De motie is uiteindelijk dan ook niet aangenomen. Wel is toegezegd een onderzoek te laten uitvoeren.

In tegenstelling tot de oppositie, was de minister van Justitie van mening dat zelf-regulering door het bedrijfsleven wel voldoende was. Daarnaast voorzag hij praktische problemen bij de strafbaarstelling: “Zolang ik niet weet dat gegevens via hacken in handen van een ander zijn gekomen, kan ik geen aangifte doen van het feit dat degene die mij had moeten waarschuwen, dat niet heeft gedaan. In alle gevallen bevinden wij ons in de sfeer van het privaatrecht. Deze kwestie wordt nu al in het economisch verkeer geregeld, namelijk via de gewone bescherming van de consument. (...) Ik denk dat dat zich geleidelijk aan ontwikkelt door zelfregulering, en op dit moment adequaat wordt gedekt."[1]

Regeringspartijen sloten zich hierbij aan:
- een meldplicht hoort thuis bij het ministerie van Economische Zaken, niet Justitie;
- een nieuwe wet past niet in het streven naar minder bureaucratie en zo min mogelijk verplichtingen voor het bedrijfsleven;
- het is beter eerst de precieze risico’s van hacking op een rij te zetten, voor invoering van een meldplicht wordt overwogen.

De Consumentenbond juichte meer druk op bedrijfsleven toe, maar vond een wet die melding verplicht ook ‘niet echt nodig’[2]. Ook de Consumentenbond was van mening dat bedrijven open moesten zijn over veiligheidsinbreuken, zodat consumenten hiermee rekening kunnen houden wanneer ze een bedrijf kiezen om mee in zee te gaan.

5.2 Vormgeving meldplicht in Nederland: meningen van experts

Mede naar aanleiding van de ontwikkelingen op Europees niveau is het onderwerp meldplicht in 2008 opnieuw opgepakt.

5.2.1 Discussie niet uitgekristalliseerd

De TV-documentaire die Zembla in november 2008 uitzond, heeft het melden van gegevensverlies onder de aandacht gebracht van media en publiek. Uit het onderzoek komt naar voren dat in Nederland de discussie over invoering van een meldplicht nog niet breed wordt gevoerd. Ze beperkt zich voornamelijk tot de overheid en organisaties als de OPTA, het CBP en de VNO-NCW. Ideeën over de inhoudelijke invulling en vormgeving van een meldplicht als wanneer en aan wie melden, hoe en door wie handhaven zijn nog niet uitgekristalliseerd. De discussie focust vooral op het doel en de effectiviteit van een meldplicht.

Uitblijven grote dataschandalen
Het uitblijven van grote dataschandalen ligt mogelijk ten grondslag aan de relatief geringe aandacht voor de meldplicht. Anders dat in de Verenigde Staten, Duitsland en het Verenigd Koninkrijk zijn in Nederland geen omvangrijke dataschandalen bekend geworden waarbij grote aantallen gevoelige persoonsgegevens verloren zijn gegaan.

[1] c) 2005, VirusAlert, ‘PvdA en SP klant informeren na hack’ (27 september 2005)
[2] Idem

5.2.2 Meldplicht met name positieve effecten op gedrag bedrijven

Doel
De geïnterviewde Nederlandse experts zijn van mening dat een meldplicht niet geschikt is om burgers een mogelijkheid te bieden maatregelen te treffen na verlies van hun gegevens. Vaak komt het verlies juist aan het licht na geleden schade. Dit geldt met name bij identiteitsfraude omdat dit slechts achteraf is vast te stellen. Feitelijk rest de consument alleen het blokkeren van een pinpas of creditcard. In de praktijk echter nemen financiële instellingen deze maatregel vaak zelf zodra een veiligheidsbreuk bij hen bekend wordt.
Het is volgens de experts wel van belang dat er een instantie is die de burger voorlicht over wat hij moet/kan doen in het geval zijn persoonsgegevens in onbevoegde handen zijn geraakt.

Omdat zij vaker op de hoogte worden gesteld van veiligheidsinbreuken, helpt een meldplicht mogelijk wel de consument bewust te maken van de risico's van bijvoorbeeld het uitwisselen van gegevens op internet. Verder kan hij naar aanleiding van meldingen besluiten een andere leverancier te kiezen. Aan de andere kant kan een teveel aan meldingen ongerustheid of juist onverschilligheid in de hand werken.

Verder biedt een meldplicht mogelijk meer inzicht in de aard en de mate van voorkomen van veiligheidsinbreuken bij overheid en bedrijven. Momenteel is hier weinig over bekend.

De respondenten zien een meldplicht vooral als een instrument om organisaties te stimuleren meer aandacht te besteden aan beveiliging. Dit omdat ze beducht zouden zijn voor imagoschade die een melding met zich meebrengt en de mogelijke markt- en/of financiële gevolgen daarvan. Volgens enkele experts heeft een systeem van vrijwillige melding of zelfregulering weinig zin omdat organisaties vanwege deze gevolgen niet erg meldingsgeneigd zullen zijn. Dit, temeer daar in Nederland privacybescherming geen 'product' is waarop organisaties met elkaar concurreren.

Doelgroep
De meeste geïnterviewde experts vinden dat een meldplicht voor zowel overheid als bedrijfsleven zou moeten gelden.

De respondenten zijn vrijwel unaniem van mening dat overheidsorganisaties met grote registers kwetsbaar zijn. Over de noodzaak van een meldplicht voor de private sector is het beeld wat genuanceerder. Een enkeling wijst erop dat de telecomsector – gezien zijn kwetsbaarheid en centrale positie – sowieso in aanmerking komt voor een meldplicht. Weer een ander merkt op dat een meldplicht voor het MKB meer van belang is dan voor bijvoorbeeld grote bedrijven in de financiële sector en grote providers in de telecomsector. Laatstgenoemde zouden hun veiligheid goed op orde hebben, terwijl in het midden- en kleinbedrijf met name vanwege de kosten de veiligheid minder prioriteit heeft. Tevens wordt gewezen op de kwetsbaarheid van toeleveranciers van bedrijven in de financiële sector (bijvoorbeeld dataopslagbedrijven) en grote winkelketens.

Sommige experts betwijfelen of organisaties hun beveiliging naar aanleiding van de meldplicht willen en kunnen aanscherpen. Respondenten verwachten dat met name kleine bedrijven niet kapitaalkrachtig genoeg zijn om te investeren in beveiliging.

5.2.3 Vormgeving

Meldplicht losstaand of als onderdeel van een bredere systematiek?
Sommige experts zijn van mening dat een meldplicht weinig effectief is als ze geen onderdeel uitmaakt van een omvattende veiligheidssystematiek die kan bestaan uit de volgende elementen.

- Duidelijke eisen waaraan een veilig systeem moet voldoen;
- Verplichte EDP-audits al dan niet gekoppeld aan een certificaat. Indien een organisatie als meldplichtig is aangewezen, zou de preventie moeten worden aangescherpt en EDP-audits verplicht. Volgens de geïnterviewde experts zouden de audits gekoppeld kunnen worden aan een keurmerk of certificaat, zoals in Duitsland het geval is. Als een organisatie beschikt over een certificaat, zou deze minder snel hoeven te melden. Geen certificaat betekent dan: altijd melden.

Anderen brengen hier tegenin dat het niet wenselijk is door middel van de meldplicht eisen te stellen aan informatiebeveiliging. Een *beveiligings*plicht is iets anders dan een *meld*-plicht. De Nederlandse wetgeving stelt al eisen aan de beveiliging van gegevens: zowel de Wet Bescherming Persoonsgegevens als de Telecommunicatiewet bevatten een beveiligingsplicht.

Flankerend beleid
Enkele Nederlandse respondenten stellen dat invoering van een meldplicht gepaard zou moeten gaan met flankerend beleid:

- Oprichting centrale instantie waar slachtoffers van identiteitsfraude terecht kunnen door bijvoorbeeld het bestaande agentschap van het ministerie van BZK te verstevigen door overheidsbrede samenwerking;
- Introductie 'fraudeer-mij-niet' register naar voorbeeld van o.a. het CIFAS-register in het Verenigd Koninkrijk;
- Instellen klokkenluiderregeling of het aanstellen van een interne privacy commissaris bij organisaties;
- Uitbreiding van de opsporingscapaciteit van hackers bij de politie;
- Uitbreiding van de handhaving/toezicht capaciteit bij de OPTA.

CIFAS-register: fraudeer mij niet
In het Verenigd Koninkrijk kunnen burgers die slachtoffer zijn geworden van ID-fraude zich aanmelden bij een anti-fraude register, het CIFAS. Bij dit register zijn veel organisaties uit de bancaire, telecom- en postsector aangesloten. Als een burger zich heeft aangemeld bij dit register, mogen deze organisaties zijn gegevens niet zomaar wijzigen. Om verder misbruik door fraudeurs te beperken, worden betalingen en de wijziging van persoonsgegevens van de getroffen burger strenger beveiligd door extra toegangscodes en paswoorden.

Voor meer informatie: www.cifas.org.uk

Grondslag voor melding
Over wanneer zou moeten worden gemeld hebben de respondenten in het algemeen nog geen uitgekristalliseerde ideeën. Eén van hen vindt dat gemeld moet worden nadat is gebleken dat onbevoegden toegang hebben gehad tot een systeem met persoonsgegevens, zonder dat aangetoond behoeft te zijn dat deze gegevens ook daadwerkelijk zijn gestolen. Een ander zou de grondslag willen leggen bij een minimum aantal verloren gegevens. Alleen bij een ernstige inbreuk zou moeten worden gemeld.

In de Verenigde Staten is het al dan niet 'encrypted' zijn van data een element van de grondslag: (mogelijk) verlies van versleutelde data behoeft dan niet te worden gemeld. Een aantal Nederlandse respondenten is hier kritisch over: de-encryptie is immers altijd mogelijk. Aan de andere kant zien respondenten wel wat in het argument dat eisen aan encryptie organisaties mogelijk stimuleren hun data door encryptie te beveiligen.

5.2.4 Handhaving en toezicht

Omdat de geïnterviewde experts verwachten dat organisaties zich niet altijd aan de meldplicht houden, hechten zij veel waarde aan handhaving en toezicht. Belangrijke redenen voor niet-naleving zijn de eerder genoemde imago (en markt en/of financiële) schade en de kosten van beveiliging en melding.

Handhavingsinstrumenten
Experts noemen de volgende mogelijkheden om de meldplicht te handhaven:
- Boetebevoegdheid toezichthouder
- Naming & shaming achteraf in geval van niet-melden door toezichthouder
- Verplichte EDP-audits door forensische accountants / toezichthouder (zie ook hierboven)

Boete: meningen verdeeld
De meningen over het nut en de noodzaak van een boete zijn verdeeld. Een aantal experts vindt dat op het niet melden van een veiligheidsinbreuk een flinke boete zou moeten staan, bijvoorbeeld onder de Wet Economische Delicten. Het percentage van de boete (bv. 10% van de omzet) kan afhankelijk zijn van de soort gegevens die de organisatie beheert. Anderzijds vragen respondenten zich af of een boete wel nuttig en terecht is. Zij zijn van mening dat een boete afdoet aan de meldingsbereidheid van bedrijven. Daarnaast geeft een boete organisaties de mogelijkheid hun meldplicht 'af te kopen'. Een expert stelt de uitbreiding van de opsporingscapaciteit van de politie als voorwaarde voor de invoering van een meldplicht.

Toezicht
Uit de interviews met experts komen verschillende alternatieven voor organisaties die toezicht moeten houden naar voren. Men is het erover eens dat er geen nieuwe organisatie voor in het leven moet worden geroepen. Respondenten opperen de volgende mogelijkheden:
- Wanneer de doelgroep van de meldplicht wordt beperkt tot telecomsector: OPTA
- Wanneer de meldplicht van toepassing is op meerdere doelgroepen:
  - CBP
  - Samenwerking OPTA en CBP
  - Toezichthouder per sector: OPTA, DNB en andere sectorale toezichthouders
  - Toezicht door Justitie: Openbaar Ministerie, parket-generaal, staatsbeveiligingsorganisatie

Aandachtspunt: capaciteit toezichthouder
Respondenten brengen de capaciteit van de toezichthouder als aandachtspunt naar voren. De benodigde capaciteit is voor een belangrijk deel afhankelijk van de reikwijdte en de grondslag van de meldplicht. In het geval van een meldplicht die voor meer organisaties geldt dan alleen de telecomsector, is het volgens respondenten van belang te waarborgen dat een toezichthouder over voldoende middelen beschikt om goed kunnen te handhaven.

Om te voorkomen dat een toezichthouder wordt overspoeld met meldingen en de meldplicht handhaafbaar te houden, is een aantal respondenten van mening dat de verantwoordelijkheid voor het bepalen of melding van een veiligheidsinbreuk (aan burgers) nodig is in eerste instantie bij de organisaties zelf moet liggen. De toezichthouder zou hier niet mee moeten worden belast.

Rol Justitie
Volgens een expert zou een melding in geval van onrechtmatige toegang altijd bij Justitie moeten worden neergelegd. Andere experts stellen dat de toezichthouder pas naar de rechter zou moeten stappen als een organisatie zich niet aan de meldplicht blijkt te houden. GOVcert of NAVI zouden de veiligheidsinbreuken achteraf kunnen evalueren, oppert een respondent.

Naleefkosten
Een aantal geïnterviewde experts vreest dat een meldplicht hoge kosten en administratieve lasten met zich meebrengt, zowel voor bedrijven als de toezichthouder. Met name kleine bedrijven en het CBP zouden deze kosten en lasten niet op kunnen brengen. Experts denken dat te hoge kosten het draagvlak voor een meldplicht bij organisaties ondermijnt. Het is daarom belangrijk dat een eventuele meldplicht kostenefficiënt wordt ingericht.

Een jaarlijks rapport als handhavinginstrument, zoals wordt voorgesteld door de EU, vinden respondenten om deze reden geen goede optie. Een dergelijk rapport levert met name een administratieve last op, voor zowel organisaties als de toezichthouder. Hier komt bij dat het niets toevoegt aan hetgeen al bekend is.

5.2.5 Samenwerking tussen overheid en private sector

Een respondent hecht waarde aan samenwerking tussen bedrijfsleven en overheid in het kader van de vormgeving en uitvoering van de meldplicht. Zoals momenteel al op eigen initiatief door het NICC[1] gebeurt, zouden overheid en het bedrijfsleven samen moeten werken om de meldplicht goed te doen functioneren en de beveiliging van persoonsgegevens te verbeteren. Vanuit dit perspectief gezien zou vrijwillige melding wenselijker zijn dan een top-down, opgelegde meldplicht.

Bij de uitvoering vindt een respondent het van belang dat organisaties samen met de toezichthouder de noodzaak en de manier van melding bepalen. Zo kan worden voorkomen dat een toezichthouder op eigen initiatief een veiligheidsinbreuk via bijvoorbeeld de website aan de consument meldt, waardoor onnodig imagoschade ontstaat.

[1] Het NICC is een publiek-privaat samenwerkingsverband tegen cybercrime, aangestuurd door het ministerie van EZ. Zie website NICC voor meer informatie, http://www.samentegencybercrime.nl/

5.3 Belangrijkste aandachtspunten voor Nederland samengevat

De elementen die een rol spelen in de besluitvorming over de invoering van een meldsysteem zijn samengevat in het model in hoofdstuk 4. Deze paragraaf vat de belangrijkste aandachtspunten samen die de geïnterviewde Nederlandse experts naar voren hebben gebracht voor Nederland.

Doelstelling

- De respondenten zien een meldplicht vooral als een instrument om organisaties te stimuleren meer aandacht te besteden aan beveiliging.

Doelgroep

- De meeste geïnterviewde experts vinden dat een meldplicht voor zowel overheid als bedrijfsleven zou moeten gelden.

Handhaving en toezicht

- Omdat de geïnterviewde experts verwachten dat organisaties zich niet altijd aan de meldplicht houden, hechten zij veel waarde aan handhaving en toezicht. Belangrijke redenen voor niet-naleving zijn de imago (en markt en/of financiële) schade en de kosten van beveiliging en melding.
- Uit de interviews met experts komen verschillende alternatieven voor organisaties die toezicht moeten houden naar voren (OPTA, CBP, sectorale toezichthouders). Men is het erover eens dat er geen nieuwe organisatie voor in het leven moet worden geroepen.
- De capaciteit van de toezichthouder is volgens de respondenten een aandachtspunt. In het geval van een meldplicht die voor meer organisaties geldt dan alleen de telecomsector, is het volgens respondenten van belang te waarborgen dat een toezichthouder over voldoende middelen beschikt om goed kunnen te handhaven.

Effecten

- Volgens de geïnterviewde Nederlandse experts heeft een meldplicht alleen effect als het sluitstuk is van een omvattende systematiek die duidelijke eisen bevat voor het beveiligen van systemen met persoonsgegevens. Als de kwaliteit van de beveiliging van persoonsgegevens goed is, wordt ook schade voor burgers verkleind.

Deel II Case-studies

- Landen met meldplicht
- Landen met vrijwillige melding
- Landen met discussie over mogelijke invoering meldplicht

Case-studies:
landen met meldplicht

- *Breach laws* in de Verenigde Staten op federaal niveau
- *Breach laws* in 44 deelstaten in de Verenigde Staten
- Californië
- Nevada
- Noorwegen

6 Breach laws op federaal niveau

De VS wordt als koploper gezien als het gaat om het invoeren van meldplicht. De onderliggende aanleiding voor het invoeren van een meldplicht is de toegenomen bezorgdheid over identiteitsfraude. De Verenigde Staten was het eerste land dat, op federaal niveau, een meldplicht implementeerde voor de financiële sector in 1999. Al snel volgde Noorwegen, dat een jaar later voerde als eerste in Europa een meldplicht invoerde. Tot op heden hebben geen andere Europese landen het Noorse voorbeeld gevolgd, terwijl in de Verenigde Staten sinds 2003 binnen in totaal 44 staten een meldplicht hebben ingevoerd. Ook op federaal niveau geldt nu voor meerdere sectoren en organisaties een meldplicht.

Deze case study beschrijft kort drie verschillende wetten op federaal niveau in de Verenigde Staten die een meldplicht bevatten, de invloedrijke Gramm-Leach-Bliley Act (2), de Veterans Affairs Information Security Act (3) en de Office of Management and Budget Guidance (4). Momenteel vinden op federaal niveau discussies plaats over een overkoepelende meldplicht (5).

Om rekening mee te houden

Wanneer we de meldplicht in de Verenigde Staten vergelijken met (discussies over) een meldplicht in andere landen is het belangrijk rekening te houden met een aantal verschillen:

- *Federale staatsstructuur* In de Verenigde Staten bestaat zowel op federaal als staatsniveau wetgeving die melding van veiligheidsinbreuken verplicht. De wetgeving op federaal niveau kan verschillen van die van de staten; ook kan de meldplicht per staat andere elementen bevatten.
- *Andere privacy wetgeving* De meeste landen in Europa hebben de bescherming van privacy vastgelegd in een wet, waarin de ver- en bewerking van persoonsgegevens wordt gereguleerd. In de VS is de bescherming van persoonsgegevens niet vastgelegd in een overkoepelende wet, maar in federale wetten van toepassing op een aantal sectoren.
- *Geen toezicht* De Verenigde Staten kent geen toezichthouder die de privacy wetgeving handhaaft, zoals de landen in Europa en Canada en Australië data of privacy autoriteiten kennen.

6.1 Zorgen om identiteitsfraude

De invoering van een meldplicht op federaal niveau en door de staten is een reactie op de toegenomen bezorgdheid over identiteitsfraude. Volgens de Federal Trade Commission gaan de meeste klachten in alle 50 staten over dit onderwerp (zie box). De bezorgdheid is het gevolg van een reeks omvangrijke dataschandalen. Voorbeelden van dataschandalen die veel media-aandacht genereerden, zijn de diefstal van een harddisk met daarop 26,5 miljoen persoonsgegevens van veteranen in 2006 en een inbreuk in het computer network van warenhuis TJX waarbij 46,2 miljoen creditcard gegevens gevaar liepen in 2007.

Bezorgdheid in cijfers
'According to the Federal Trade Commission, identity theft is the most common complaint from consumers in all 50 states, and accounts for over 35% of the total number of complaints the Identity Theft Data Clearinghouse received for calendar years 2004, 2005, and 2006. In calendar year 2006, of the 674,354 complaints received, 246,035 or 36% were identity theft complaints'[1].

Vanwege minder strikte privacy wetgeving en het wijdverbreide, commerciële gebruik van de Amerikaanse versie van het sofinummer, het *social security number* (SSN), zijn Amerikaanse burgers vatbaarder voor schade bij verlies van persoonsgegevens. Bedrijven in Europa mogen bijvoorbeeld de elektronische gegevens of e-mail van een consument pas gebruiken voor reclamedoeleinden wanneer de consument hier expliciet toestemming heeft gegeven. Bedrijven in de VS mogen elektronische gegevens altijd gebruiken, mits de consument zijn 'toestemming' intrekt. Het SSN, daarnaast, wordt niet alleen gebruikt door de overheid, maar ook voor commerciële doeleinden door het bedrijfsleven. Het SSN verleent dus niet alleen toegang tot dossiers bij overheidsinstanties, zoals dat in Nederland het geval is, maar ook tot krediet en rekeningen. Voor criminelen is het SSN daarom een populair doelwit.

Hoewel er geen empirisch bewijs is dat een meldplicht identiteitsfraude beperkt of voorkomt, wordt de invoering van een meldplicht vanwege de bezorgdheid over ID-fraude over het algemeen breed gedragen in de Verenigde Staten.

6.2 Federale *breach laws:* sectorale aanpak[2]

Op federaal niveau bestaat geen overkoepelende wet die de bescherming van alle soorten gevoelige persoonsgegevens voor zowel de overheid als het bedrijfsleven reguleert. De federale overheid hanteert een *sectorale* aanpak. Per sector zijn richtlijnen geïmplementeerd die bepaalde organisaties verplichten om informatie goed te beveiligen en veiligheidsinbreuken te melden aan de betrokkenen. Het gaat om de financiële sector, gezondheidszorg, overheid, beveiliging- en internetsector. Binnen de private sector zijn weer verschillende wetten van toepassing voor verschillende sectoren. Belangrijke wetten op het gebied van privacy bescherming en data beveiliging zijn:

Voor de federale overheid:
Privacy Act;
Federal Information Security Management Act;
Office of Management and Budget Guidance (OMG);
Veterans Affairs Information Security Act

Voor de private sector:
Health Insurance Portability and Accountability Act (HIPAA);
Gramm-Leach-Bliley Act;
Federal Trade Commission Act;
Fair Credit Reporting Act.

[1] Een belangrijke en zeer nuttige bron over federale *breach laws* in de Verenigde State is het rapport CRS Report for Congress: Federal Information Security and Data Breach Notification Laws (3 april 2008) geschreven door Gina Marie Stevens Legislative Attorney (CRS, Order Code RL34120)
[2] Idem

De wetten vereisen allemaal een adequate beveiliging van persoonsgegevens; een aantal van deze wetten bevatten ook een meldplicht. De invulling, soort gegevens en handhaving van de meldplicht verschilt echter per wet.

Voor- en tegenstanders sectorale aanpak[1]
Volgens critici heeft de sectorale aanpak als nadeel dat de huidige federale wetten meer focussen op de manier waarop een bepaalde sector informatie gebruikt (b.v. medische gegevens), dan op de bescherming van de privacy van burgers. Voorstanders van de sectorale aanpak vinden het juist goed dat de wetten rekening houden met sector specifieke eigenschappen en verschillende soorten informatie. Anderen pleiten voor een nationale standaard voor organisaties die persoonsgegevens beheren zodat verschillende richtlijnen worden geharmoniseerd.

In het vervolg van deze paragraaf worden kort twee federale wetten en een richtlijn die een meldplicht bevatten, besproken; de Gramm-Leach-Bliley Act, de Veterans Affairs Information Security Act en de Office of Management and Budget Guidance.

6.3 Gramm-Leach-Bliley Act (GLBA)

De Gramm-Leach-Bliley Act uit 1999, van toepassing op de financiële sector, was de eerste wet ter wereld waarin een meldplicht werd opgenomen. Deze wet heeft dan ook grote invloed gehad op de ontwikkeling van een meldplicht in de Verenigde Staten. In hoofdstuk 5 van de Act wordt gesteld dat financiële instellingen (o.a. banken, verzekeraars en effecten fondsen) de persoonsgegevens van hun klanten voldoende moeten beschermen tegen inbreuken, onbevoegde toegang en onbevoegd gebruik. De gedetailleerde richtlijnen aan de hand waarvan deze eis wordt geïmplementeerd, bevelen financiële instellingen aan een response programma te implementeren om goed te kunnen omgaan met veiligheidsinbreuken, *Response Program for Unauthorized Access to Customer Information and Customer Notice.*

Response program = meldplicht
De *response programs* moeten procedures bevatten voor het melden van een inbreuk. De grondslag voor melding is tweeledig: (1) onbevoegde toegang of gebruik van klantgegevens is geschied en kan leiden tot substantiële schade ‘or inconvenience’ voor klanten, en (2) als de financiële instelling die deze gegevens beheert van mening is dat misbruik van de informatie heeft plaatsgevonden of dat misbruik redelijkerwijs mogelijk is.

Procedure
Een *response program* moet minimaal procedures bevatten voor een onderzoek naar de aard en reikwijdte van een inbreuk en om welke informatie het gaat. Als de instelling op basis van het onderzoek vindt dat de verkregen informatie is of zal worden misbruikt, moet deze de klant zo snel mogelijk op de hoogte stellen. Ook moet de financiële instelling de inbreuk melden aan de federale toezichthouder (FTC) en justitie. De melding aan klanten mag niet worden uitgesteld, tenzij het om gegevens gaat die nodig zijn voor justitieel onderzoek naar een misdrijf. Tot slot moet het *response program* omschrijven welke stappen de financiële instelling neemt om een inbreuk te beperken, hoe zij verdere onbevoegde toegang voorkomt en wanneer zij de klanten op de hoogte zal stellen.

[1] Idem

6.4 Veterans Affairs Information Security Act

De Veterans Affairs Information Security Act werd geïmplementeerd na een hack van een computer bij een veteraan thuis in 2006, waarbij de hacker toegang had gekregen tot de persoonsgegevens van 26,5 miljoen veteranen[1]. De wet schrijft voor dat de Veterans Administration (VA) veiligheidsprocedures implementeert om de persoonsgegevens van veteranen en de informatiesystemen te beschermen[2]. Een onderdeel van de veiligheidsvoorschriften is een meldplicht in geval van een *data breach* van gevoelige persoonsgegevens die worden verwerkt en opgeslagen door de secretaris van de VA.

Procedure
De grondslag van melding is de mate van mogelijk misbruik van de persoonsgegevens. Onmiddellijk na het ontdekken van een veiligheidsinbreuk, moet de secretaris van de Veterans Administration (VA) een onafhankelijke risicoanalyse laten uitvoeren door een externe organisatie of de VA inspecteur. Als de secretaris op basis van deze analyse van mening is dat er redelijkerwijs sprake is van mogelijk misbruik, moet hij zorgdragen voor de bescherming van het krediet van de veteranen. Daarnaast moet hij de resultaten van elke risicoanalyse en de ondernomen acties rapporteren aan de Veterans Committee van de senaat[3]. Als de gegevens informatie bevatten over een overleden burger of legerpersoneel, moet de secretaris de inbreuk ook melden aan de Armed Services Committee van de senaat[4]. Ter aanvulling moet de secretaris elk kwartaal rapporteren over alle veiligheidsinbreuken en verlies van gevoelige gegevens aan de Veterans Committees van het Congres.

6.5 Office of Management and Budget Breach Notification Policy

Bij wijze van reactie op de aanbevelingen van de Identity Theft Task Force van de President[5], bracht het Office of Management and Budget (OMB)[6] in mei 2007 een memorandum uit over 'Safeguarding Against and Responding to the Breach of Personally Identifiable Information'[7]. Het memorandum schrijft voor dat alle federale overheidsorganisaties een meldplicht moeten implementeren[8]. De meldplicht geldt voor persoonsgegevens in zowel papieren als digitale vorm.

Het Office of Management and Budget (OMB) assisteert de President bij de voorbereiding van de federale begroting en coördineert het regeringsbeleid op het gebied van financiën en informatie.

Procedure
De grondslag voor melding is de mate van 'likely risk of harm'. Elke federale overheidsorganisatie moet een 'agency response team' instellen dat de veiligheidsinbreuk aan moet pakken. Na ontdekking van een veiligheidsinbreuk moet er binnen een uur *intern* melding worden gemaakt. Om te bepalen of de inbreuk ook *extern* moet worden gemeld, moet de orga-

[1] Meer informatie over deze hack op de US government website: http://www.usa.gov/veteransinfo.shtml
[2] Veterans Affairs Information Security Act. Title IX of P.L. 109-461.
[3] Website Veterans Committee: http://veterans.senate.gov/public/
[4] Website Armed Services Committee: http://armed-services.senate.gov/about.htm
[5] Voor meer informatie, zie website Task Force: http://www.idtheft.gov/
[6] Idem
[7] OMB Memorandum M-07-16
[8] Attachment 2 van het OMB Memorandum, Incident Reporting and Handling Requirements

nisatie rekening houden met een aantal factoren[1]. Als melding nodig wordt geacht, moet dit zo snel mogelijk gebeuren. Uitstel is geoorloofd als een justitieel onderzoek naar een misdrijf, de nationale veiligheid of 'agency needs' dit vereisen. Het memorandum stelt dat melding van versleutelde (encrypted) informatie niet altijd nodig is. Het memorandum bevat verder criteria voor de manier waarop de veiligheidsinbreuk aan burgers wordt gemeld.

Veiligheidsmaatregelen vereist

Om te komen tot een meldplicht moeten organisaties eerst hun privacy en veiligheidsbeleid onder de loep nemen. Ook moeten zij vijf nieuwe veiligheidsmaatregelen treffen:

- encryptie van alle data op mobiele apparaten als laptops en memorysticks;
- toepassen van 'two-factor authentication' voor toegang tot het systeem op afstand;
- toepassen van een 'time-out' functie voor toegang tot het systeem op afstand;
- vastleggen en checken van alle voor de computer leesbare data opgeslagen in databases met gevoelige informatie;
- opstellen van een jaarlijks te ondertekenen intentieverklaring voor personen die toegang hebben tot persoonsinformatie met daarin hun verantwoordelijkheden.

6.6 Een federale meldplicht voor alle sectoren?

Mogelijk wordt op federaal niveau een overkoepelende meldplicht ingevoerd. Tijdens het 110e Congres in 2008 stelden drie Commissies van de Senaat elk verschillend ingerichte data beveiligingswetgeving voor, met daarin een meldplicht, S. 239 (Feinstein), S. 495 (Leahy) en S. 1178 (Inouye)[2]. Tot op heden is een overkoepelende meldplicht om een aantal redenen nog niet tot stand gekomen.

Opschorting federale meldplicht om vier redenen

Ten eerste kunnen de commissies het niet met elkaar eens worden over bepaalde elementen van de meldplicht, zoals voor wie de meldplicht moet gelden en hoe deze moet worden gehandhaafd. Het belangrijkste twistpunt is echter de grondslag voor melding. Daarnaast is de noodzaak voor een overkoepelende meldplicht afgenomen nu 44 staten deze zelf al hebben ingevoerd. Verder heeft de regering momenteel meer aandacht voor problemen met medische dossiers dan veiligheidsinbreuken in het algemeen. Een vierde, belangrijke reden voor de opschorting van de federale meldplicht is dat financiële instellingen geen aanvullende regelgeving wensen, omdat voor hen al een meldplicht geldt onder de Gramm-Leach-Bliley Act. In geval van een overkoepelende meldplicht eisen zij 'safe harbour', ofwel dat nieuwe eisen niet voor hen gelden.

Wat nu?

Het is niet bekend wanneer een federale meldplicht door de nieuwe regering weer op de agenda wordt gezet. Indien de meldplicht er wel komt, komt er geen overkoepelende, nieuwe wet. De sectorale wetten die al een meldplicht bevatten, zouden kunnen worden aangepast aan de nieuwe eisen. Daarnaast zal een meldplicht worden opgenomen in federale wetgeving die nog geen meldplicht bevat.

[1] Attachment 3 van het OMB Memorandum, External Breach Notification

[2] CRS Report for Congress: Federal Information Security and Data Breach Notification Laws (3 april 2008) geschreven door Gina Marie Stevens Legislative Attorney (CRS, Order Code RL34120).

To pre-empt or not to pre-empt

De vraag of een federale wetgeving de meldplichten op het niveau van de staten moet harmoniseren of ontkrachten (pre-emption) lijkt geen belangrijk issue te zijn in de discussie. De verwachting is dat de staten geen voorstander zullen zijn van pre-emption, omdat zij hun eigen meldplicht willen behouden.

Op federaal niveau wordt veel belang gehecht aan de 'kraamkamer-functie' van de staten, waardoor pre-emption of harmonisatie weinig prioriteit heeft. Staten worden gezien als de 'incubators of democracy': zij weten het beste welke wetgeving in hun situatie het meest geschikt is. Dat grote bedrijven rekening moeten houden met 44 verschillende meldplichten, wordt niet gezien als een probleem. Bedrijven zijn hier al aan gewend, omdat staten op allerlei gebieden verschillende wetgeving hebben geïmplementeerd. Bovendien zijn de meldplichten op staatsniveau in essentie grotendeels hetzelfde[1].

[1] Bronnen interviews respondenten federaal niveau.

7 *Breach laws* in deelstaten

In de Verenigde Staten sinds 2003 binnen in totaal 44 staten een meldplicht hebben ingevoerd. De wetgeving is niet in alle staten hetzelfde vormgegeven.
Deze casestudy biedt een globaal overzicht van de mogelijke keuzes die de staten hebben gemaakt.

Deze paragraaf is grotendeels gebaseerd op de nuttige overzichten van Pam Greenberg (NCSL) en Julie Brill (Officier van Justitie, Vermont). Deze experts houden de ontwikkeling van en verschillen tussen meldplichten op deelstaatniveau nauwkeurig bij.

7.1 Vormgeving

Voor welke organisaties?
De meeste staten in de VS hebben gekozen voor een meldplicht personen en organisaties die binnen de grenzen van de staat of het land *werkzaam* zijn[1]. Hierbij wordt geen onderscheid gemaakt tussen het bedrijfsleven als (semi-)overheid. Het gevolg is dat bedrijven die niet in de staat zelf zijn gevestigd zich ook aan de meldplicht van de staat moeten houden. Slechts enkele staten in de VS wijken van de standaard af.

Afwijken van de standaard
Georgia en Maine hebben een meldplicht die geldt voor 'data brokers' (bedrijven die in opdracht databases doorzoeken en de gevraagde informatie aanlevert). In Indiana, Nevada en Vermont geldt de meldplicht voor alle 'data collectors' (alle organisaties die persoonsgegevens verzamelen, ver- of bewerken en beheren). Een aantal staten maken een uitzondering voor financiële instellingen of zorgorganisaties die vallen onder federale wetgeving. In enkele gevallen is de meldplicht voor bedrijven in een andere wet opgenomen dat voor overheden. Dit is bijvoorbeeld het geval in Californië en Indiana.

Soort gegevens
In de Verenigde Staten geldt de meldplicht op deelstaatniveau voor persoonsgegevens. Persoonsgegevens zijn gewoonlijk gedefinieerd als:

'An individual's first name or first initial and last name, in combination with any one or more of national ID number, drivers license number, medical information or financial account number, combined with any required security or access code or password that would permit access to an individual's financial account'[2].

Veel staten maken een uitzondering voor openbare informatie waarvan het wettelijk is toegestaan dat zij openbaar zijn gemaakt. Hiermee worden gegevens bedoeld uit openbare overheidsdatabases of media.

Een trend in de Verenigde Staten is om medische gegevens expliciet onder de meldplicht laten vallen, zoals Californië onlangs heeft gedaan. De federale wet die voor de gezond-

Arkansas heeft expliciet ook 'fysieke' gegevens aan de meldplicht toegevoegd; North Carolina heeft het over 'written, drawn, spoken, visual or electromagnetic personal information'.

[1] Security breaches chart Julie Brill, en overzicht Consumer's Union uit 200
[2] Dr. Demi Getschko, Malcolm Harbour, Henry L. Judy, David Satola, Rajne
net Governance Forum (Rio de Janeiro Brazil, November 2007) getiteld: C
Protection and Data Breach Notification en overzicht Julie Brill.

heidszorg geldt, HIPAA, is namelijk niet expliciet over veiligheidsinbreuken van medische gegevens.

Digitaal of ook papier?
In de meeste staten in de VS is de meldplicht alleen van toepassing op computerized gegevens en sluiten papier uit van de meldplicht. Gewoonlijk wordt onder 'computerized' digitale of elektronische gegevens verstaan.

Versleuteld of niet?
Bijna zonder uitzondering kiezen de deelstaten ervoor om versleutelde gegevens uit te sluiten van de meldplicht. Er wordt ten eerste vanuit gegaan dat het risico op schade kleiner is als de gegevens zijn versleuteld. Daarnaast is dit een van de manieren waarop overheden organisaties proberen te stimuleren meer aandacht aan beveiliging te schenken, met name aan de beveiliging van *carry on media.* Na invoering van de meldplicht in Californië bleek namelijk dat veel inbreuken het gevolg waren van gestolen laptops en memoriesticks met informatie die niet was beveiligd.

Grondslag voor melding
In de Verenigde Staten wordt naar het voorbeeld van Californië meestal gekozen voor de drempel *acquisition of data* of een zekere vorm van schade voor de betrokkenen. Enkele staten leggen de lat lager en vereisen melding zodra er een veiligheidsinbreuk heeft plaatsgevonden. De meeste deelstaten kiezen hier niet voor, waarschijnlijk omdat zij van mening zijn dat dit nodeloos angst inboezemt bij consumenten. Het risico op identiteitsfraude wordt ook als grondslag gebruikt, maar minder vaak. Het aantal verloren gegevens of gedupeerden wordt vrijwel nooit als grondslag gebruikt; het verlies van creditcardgegevens kan voor 1 persoon immers al erg schadelijk zijn.

***Acquisition of data* of *likelihood of harm*?**
Om de complexiteit van het bepalen van de grondslag te illustreren, noemen we hier als voorbeeld de tegengestelde mening van Californië en Australië over twee grondslagen.

Californië heeft gekozen voor *acquisition of data.* Het feit dat een hacker toegang tot gegevens heeft gekregen, is immers en indicatie van mogelijke schade. De trigger *likelihood of harm,* dat sommige staten hanteren, is volgens het *Office of Privacy Protection* betwistbaar en subjectief: wat is schade precies? En wie bepaalt dat? Door *acquisition of data* als trigger te hanteren, kan Californië zoveel mogelijk uitgaan van de feiten bij de beslissing om te melden.

De grondslag *likelihood of harm* biedt volgens Australië echter een hogere drempel voor melding dan 'unauthorized acquisition', omdat de organisatie rekening moet houden met meerdere factoren dan alleen de vraag of de hacker toegang heeft gekregen tot gevoelige informatie. Om te bepalen of melding nodig is, zou de organisatie rekening moeten houden met de oorzaak en reikwijdte van de inbreuk, wie wordt gedupeerd en wat de mogelijke schade is. Een hogere drempel is nodig om een overvloed van meldingen aan consumenten te voorkomen.

Aan wie melden?
In de meeste staten hoeven organisaties inbreuken alleen aan de getroffen burgers te melden. De Verenigde Staten kent immers geen centrale toezichthouder die de privacy wetgeving handhaaft, zoals de landen in Europa en Canada en Australië data of privacy autoriteiten kennen. De staten Wisconsin en Californië hebben als enigen een Office of Privacy Protection, maar deze organisaties hebben geen sanctiebevoegdheden.

Als deelstaten in de VS ervoor kiezen om een instantie tussen organisatie en burger in te plaatsen, kiezen zij daarom voor justitie. In de meeste gevallen komt dit neer op de officier van justitie, die verantwoordelijk is voor de bescherming van de privacy van burgers. In dit geval dient de organisatie samen met justitie te bepalen of er risico op schade is en of melding aan de burger nodig is.

7.2 Procedure

Als een organisatie besluit de inbreuk te melden, schrijft de meldplicht in deelstaten vrijwel altijd voor dat de melding op het meest gunstige moment en zonder uitstel aan de betrokkenen wordt gemeld. De meeste deelstaten stellen gedetailleerde eisen aan de vorm en inhoud van een melding.

De melding kan verschillende vormen hebben:
- Formulier
- E-mail
- Per brief
- Telefonisch (bijvoorbeeld Georgia, Illinois, Washington)
- Fax (bijvoorbeeld Indiana)

In de Verenigde Staten geven deelstaten niet altijd de voorkeur aan een e-mail; deze kan er nep uitzien.

Omdat het doel van de meldplicht is om schade bij burgers te voorkomen, hechten deelstaten veel waarde aan het communiceren van de maatregelen die burgers kunnen treffen. Zij vinden het belangrijk dat de melding in ieder geval advies en een follow-up bevat over maatregelen die de consument kan nemen om schade te voorkomen. In de VS moet een melding gewoonlijk informatie bevatten over:
- Wat is er precies gebeurd en wanneer?
- Om welke persoonsinformatie gaat het?
- Wat heeft de organisatie zelf gedaan om de inbreuk in te perken?
- Wat doet de organisatie om toekomstige inbreuken te voorkomen?
- Waar kan de consument terecht met vragen?
- Waar kan de consument een klacht indienen?
- Welke maatregelen kan de consument nemen om schade te voorkomen?

Maatregelen?
Een voorbeeld van een maatregel is het bevriezen of blokkeren van een rekening. In de VS hebben 39 staten plus het District van Columbia wetgeving die van credit bureaus vereist om consumenten in staat te stellen hun rekeningen te beschermen door een 'security freeze' aan te vragen[1].

7.3 Wettelijk kader

In de VS heeft invoering van een meldplicht door de deelstaat vaak tot doel om de gaten op te vullen waar geen federale meldplicht geldt. Door de sectorale aanpak heeft de federale overheid (nog) niet voor alle sectoren of organisaties een meldplicht ingevoerd. Een meldplicht op staatsniveau stelt de Officier van Justitie en burgers in staat te procederen wanneer een veiligheidsinbreuk *binnen* de grenzen van de staat plaatsvindt.
De deelstaten hebben de meldplicht dan ook steeds ad hoc ingevoerd middels implementatie van een aparte *bill* of ingevoegd in een bestaande wet die van toepassing is op bedrijven of overheden in het algemeen.

7.4 Handhaving

Ex-ante handhaving door sanctioneren (achteraf) komt het meest voor in de Verenigde Staten. Op niet melden staat in een groot aantal staten in de VS een boete. Deze boete varieert van $ 2500 (b.v. Hawaii) tot $ 150.000 (b.v. New York) per inbreuk.

In de Verenigde Staten is de officier van justitie meestal verantwoordelijk voor het handhaven van de meldplicht. Hij mag daartoe rechtszaken aanspannen, medewerking van bedrijven afdwingen en een schadevergoeding eisen. In de Verenigde Staten hebben burgers in een aantal staten ook het recht op basis van de meldplicht civiele procedures aan te spannen als zij slachtoffer zijn geworden van de gevolgen van een veiligheidsinbreuk. De meldplicht mag echter niet altijd als grond dienen voor rechtelijke stappen. Dan wordt de meldplicht indirect gehandhaafd door procedures aan te spannen op basis van schending van wetgeving op gerelateerde terreinen als bescherming van consumenten, malpractice, fraude of oneerlijk handelen.

[1] Zie http://www.consumersunion.org/campaigns/learn_more/003484indiv.html

8 Californië

Wanneer ingegaan	1 juli 2003
Welke wet	Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29 (bedrijven), 1798.82 (overheden)
Doel	Het voorkomen van identiteitsfraude
Voor welke organisaties	*'Each agency, person, or business that conducts business in Californië and owns or licenses computerized data containing personal information'*
Welke soort gegevens	Niet-gecodeerde, geautomatiseerde persoonsgegevens (incl. SSN en sinds 2008 medische gegevens)
Wanneer melden	In het geval dat een organisatie weet dat er een reële mogelijkheid is dat een onbevoegd persoon persoonsgegevens heeft verworven.
Aan wie melden	Consument / burger
Handhaving	Indirect via gerelateerde wetgeving op basis waarvan burgers zelf rechtelijke stappen ondernemen tegen organisaties en bedrijven.
Toezicht	*Californië Office of Privacy Protection*: geen bevoegdheden
Bijzonderheden	Eerste staat in de Verenigde Staten die een meldplicht invoerde. Geldt door omissie niet voor lokale overheden.

8.1 Aanleiding

Californië is de eerste staat in de Verenigde Staten die in 2003 een wettelijke meldplicht instelde. De *onderliggende* aanleiding van de meldplicht was identiteitsfraude, een onderwerp dat aan veel meldplichten in de Verenigde Staten ten grondslag ligt. Wetgevers in Californië waren al enkele jaren gericht op identiteitsfraude en privacy. In de jaren voor de implementatie van de meldplicht had Californië al gerelateerde wetgeving geïmplementeerd. Een voorbeeld is wetgeving die overheidsorganisaties verplicht om privacybeleid op te stellen betreffende de persoonsgegevens die zij beheren[1].

De directe aanleiding van de invoering van een meldplicht was een succesvolle inbreuk in de server van het data centrum van de staat begin 2002, het *Stephen P. Teale Data Center*[2]. Gedurende een periode van enkele weken had een –nog altijd onbekende- hacker toegang tot vertrouwelijke informatie over 265.000 ambtenaren in dienst van de staat van Californië, inclusief ambtenaren van de wetgevende macht. Het centrum stelde de ambtenaren pas drie weken na ontdekking van de inbreuk op de hoogte. Het incident leidde tot de roep om het een wettelijke meldplicht in geval van inbreuken[3].

[1] State of California, SB 129 (Peace), 8/31/00, 40-0, Statutes of 1999.
[2] State of California, SENATE THIRD READING, SB 1386 (Peace), As Amended August 5, 2002.
[3] CRM BUYER SPECIAL REPORT: Hacking the Call Center (14 oktober 2003) http://www.crmbuyer.com/story/31817.html

8.2 Discussie

Ondanks enige tegenstand uit de ICT- en financiële sector werd invoering van een meldplicht breed gedragen in Californië. De discussie draaide niet om de vraag of er wel een meldplicht moest komen, maar om de *inhoud* van de meldplicht.

Het belangrijkste argument voor de meldplicht was dat consumenten op de hoogte gesteld moeten worden van een inbreuk, zodat zij maatregelen kunnen nemen om te voorkomen dat zij slachtoffer worden van identiteitsfraude. Voorstanders van een meldplicht als het *Privacy Rights Clearinghouse* en het *Identity Theft Resource Center* vonden het ook belangrijk dat consumenten *zo snel mogelijk* op de hoogte werden gesteld: des te sneller de consument in staat wordt gesteld te handelen, des te kleiner de kans op identiteitsfraude

Tegenstand kwam van twee organisaties uit de ICT- en bancaire sector. Het *Information Technology Association of America* (ITAA) was bezorgd over de '*piecemeal state to state regulation'* van de meldplicht. Invoering van een meldplicht hoorde volgens de ITAA thuis op federaal niveau. Het *Investment Company Institute* (ICI), een coalitie van investeringsfondsen, voorzag hoge kosten voor bedrijven die een meldplicht met zich mee zou brengen. Daarnaast zou een meldplicht bedrijven verplichten om consumenten 'nodeloos' te informeren.

Omdat er geen sprake van was dat de meldplicht niet zou worden ingevoerd, concentreerde de discussie zich op het criterium waarop melding van een inbreuk moest worden gebaseerd: ongeautoriseerde toegang tot een systeem of het verkrijgen van persoonsgegevens door een ongeautoriseerde persoon? Uiteindelijk is gekozen voor het criterium verkrijgen van persoonsgegevens.

8.3 Vormgeving

Doelgroep
De meldplicht geldt voor overheidsorganisaties op staatniveau (*state agencies*), personen en bedrijven die handelen in Californië en geautomatiseerde gegevens (*computerized data*) beheren of uitgeven waar persoonsgegevens deel van uitmaken. Door een omissie geldt de meldplicht niet voor lokale overheden.

Soort gegevens
De meldplicht geldt voor onbeveiligde of onversleutelde (*unecrypted*), geautomatiseerde (*computerized*) persoons-gegevens (*personal information*). Californië verstaat onder 'personal information' een voor- en achternaam in combinatie met het *social security number* (SSN), rijbewijsnummer, het nummer van de identiteitskaart, of een rekening-, pinpas- of creditcardnummer in combinatie met de benodigde toegangscode of wachtwoord. Vanaf 2008 is Californië één van de staten die ook medische gegevens expliciet onder de meldplicht scharen.

Opvallend is dat de wetgeving geen definitie geeft voor de term 'computerized': de betekenis van deze term is ook nog nooit aanhangig gemaakt. In het algemeen verstaat men onder 'computerized' digitale gegevens; hier vallen papieren gegevens niet onder. Het *Cali-*

fornië Office of Privacy Protection adviseert dat het medium waarop de gegevens zijn opgeslagen niet relevant is, een standpunt dat ook op overheidsniveau wordt aangehangen.

In de *praktijk* lijkt dit ook het geval: organisaties melden ook het verlies van *papieren* gegevens. Hoewel er in dit geval minder mensen worden gedupeerd, kan er immers toch sprake zijn van schade voor individuen. Verschillende pogingen om ook het verlies van papieren gegevens formeel op te nemen in de meldplicht hebben geen doorgang gevonden door tegenstand van het bedrijfsleven.

Grondslag voor melding

Californië heeft gekozen voor de '*acquisition of data*' als grondslag voor een melding. Wanneer na een inbreuk in een systeem is aangetoond dat onbeveiligde persoonsinformatie is verkregen door een ongeautoriseerde persoon, of wanneer dat dit redelijkerwijs mogelijk is, dient een organisatie de betrokken personen hier van op de hoogte te stellen. De meldplicht schrijft niet voor dat de organisatie justitie of het *Office of the Privacy Commissioner* op de hoogte moet stellen van de inbreuk.

Californië heeft expliciet niet gekozen om melding van elke veiligheidsinbreuk verplicht te stellen. Men is van mening dat dit nodeloos angst inboezemt bij consumenten. Het criterium van een minimum aantal verloren data of gedupeerden is nooit ter sprake gekomen tijdens de discussie. De grondslag *likelihood of harm,* die sommige staten hanteren, is volgens het *Office of Privacy Protection* betwistbaar. Het is moeilijk om dit criterium objectief te definiëren; de definitie en daardoor ook de melding hangt daarom af van de maatstaf die een organisatie intern hanteert. Door *acquisition of data* als grondslag te hanteren, kan Californië zoveel mogelijk uitgaan van de feiten bij de beslissing om te melden.

Op basis van de feiten

De volgende twee gevallen illustreren hoe in Californië aan de hand van het criterium *acquisition of data* wordt bepaald of een veiligheidsinbreuk wordt gemeld.

Niet gemeld

In een geval had iemand voor een langere periode de server van een organisatie gehackt. Op deze server waren naast gevoelige gegevens ook muziek en video's opgeslagen. Uit het onderzoek dat plaatsvond nadat de hack was ontdekt, bleek dat de hacker de server als opslag voor muziek en video's had gebruikt. Er was geen bewijs dat hij de gegevens had verkregen: de veiligheidsinbreuk is niet gemeld.

Wel gemeld

Bij eenzelfde soort hack toonde het bewijs aan dat de inbreuk van de server in relatie stond met een *botnet*. Daarnaast waren *log files* gewist. In dit geval kon de organisatie niet met zekerheid zeggen dat de hacker de gevoelige gegevens *niet* had verkregen. Daarom achtte men het verstandig melding te maken van de inbreuk.

8.4 Procedure

Wanneer een veiligheidsinbreuk heeft plaatsgevonden, dient de organisatie onderzoek te (laten) verrichten naar de oorzaak van de inbreuk en de handelingen die de inbreker binnen het systeem heeft verricht (*log file*). Voor zover mogelijk, wordt op basis van deze feiten

bepaald of een hacker (mogelijk) gegevens heeft verkregen en of melding moet worden gemaakt aan de consument.

Als een organisatie besluit de inbreuk te melden, schrijft de meldplicht voor dat de melding op het meest gunstige moment en zonder uitstel aan de betrokkenen wordt gemeld. Behalve als federale wetgeving anders voorschrijft, mag de organisatie de betrokkenen alleen schriftelijk op de hoogte stellen. De organisatie mag het incident alleen op een andere manier bekend maken, als zij kan aantonen dat de kosten van de melding meer dan $ 250.000 bedragen, er meer dan 500.000 mensen op de hoogte moeten worden gesteld of wanneer adresgegevens niet bekend zijn. Alleen in deze gevallen mag de organisatie melding maken via e-mail, de website of de media.

8.5 Wettelijk kader

De meldplicht voor overheidsorganisaties is opgenomen in een andere wet dan de meldplicht voor bedrijven. Bedrijven vallen onder Cal. Civ. Code §§ 1798.82. Maar de eerstgenoemde meldplicht is onderdeel van een wet die geldt voor overheden op staatsniveau, Cal. Civ. Code §§ 1798.29. Deze wet is niet van toepassing op lokale overheden, waardoor zij niet wettelijk gebonden zijn aan een meldplicht. Pogingen om lokale overheden ook in deze wet op te nemen falen; omdat het een omvangrijke wet is die veel meer onderwerpen dan alleen de meldplicht omvat, wegen voor lokale overheden de kosten van het wijzigen en implementeren van deze wet niet op tegen de baten.

In de praktijk melden lokale overheden echter wel; de meldplicht is in feite gewoonterecht geworden (common-law). De opvatting is dat het nalatig zou zijn als lokale overheden niet melden in geval van een inbreuk. Het is mogelijk dat zij minder melden dan de organisaties die wel vallen onder de meldplicht.

8.6 Handhaving en toezicht

Indirecte handhaving
Californië heeft geen onafhankelijke autoriteit die toezicht houdt op de naleving van de meldplicht. De meldplicht wordt indirect via gerelateerde wetgeving gehandhaafd op basis waarvan burgers rechtelijke stappen kunnen ondernemen tegen organisaties en bedrijven. Wanneer zij schade hebben geleden, kunnen burgers organisaties aanklagen op basis van wetgeving over oneerlijke concurrentie, privacy en de beveiliging van gegevens.

Meldplicht in combinatie met wetgeving die beveiliging en follow-up verplicht
Om verandering van gedrag van organisaties als het gaat om de beveiliging van systemen en de privacy van consumenten af te dwingen, heeft de staat Californië naast de meldplicht in 2005 ook wetgeving aangenomen die de beveiliging (*encryption*) van gegevens verplicht stelt, onafhankelijk van het medium waarop deze gegevens zich bevinden. Daarnaast moeten organisaties volgens andere wetgeving een plan voor herstel (*remediation plan)* opstellen voor klanten die zijn geschaad door een inbreuk.

Office of Privacy Protection

Samen met Wisconsin is Californië een van de weinige staten die een aparte organisatie heeft die is gespecialiseerd in privacybescherming; het *Office of Privacy Protection*[1]. In de andere staten maakt de bescherming van de privacy van consumenten deel uit van het departement van de procureur-generaal. Het *Office of Privacy Protection* van Californië heeft geen boete- of auditbevoegdheid, maar fungeert wel als meldpunt.

Het *Office* wordt geregeld gebeld door consumenten en werknemers die een inbreuk of gegevensverlies hebben geconstateerd. Wanneer een medewerker anoniem een inbreuk meldt, neemt het *Office* contact op met de organisatie in kwestie om het te wijzen op de inbreuk. Over het algemeen zijn bedrijven ontvankelijk voor dit signaal en ondernemen zij actie. Als een bedrijf weigert actie te ondernemen, kan het *Office* naar justitie stappen.

De meldplicht is ook van toepassing op gegevens van medewerkers; zij hechten dus veel belang aan het melden van inbreuken door hun organisatie.

8.7 Evaluatie

Het doel van de meldplicht is om consumenten op tijd op de hoogte te stellen van het feit dat zij risico lopen; volgens het *Office of Privacy Protection* is dit doel bereikt. Het *Office* is daarnaast van mening dat de meldplicht veranderingsprocessen binnen organisaties stimuleert. Bedrijven hebben meer aandacht gekregen voor de beveiliging van hun systemen en voor de privacy van consumenten.

In Californië zijn echter *geen gegevens* bekend over de mate van navolging van de meldplicht. Er is geen empirisch bewijs dat invoering van de meldplicht heeft geleid tot een afname van veiligheidsinbreuken of identiteitsfraude. Ook is niet bekend in hoeverre de meldplicht heeft geleid in verandering van het gedrag van organisaties als het gaat om beveiliging van systemen en privacy. Volgens het *Office of Privacy Protection* houden de meeste bedrijven en organisaties zich er wel aan. De imagoschade en hoge kosten van het melden van een inbreuk wegen immers zwaar voor bedrijven. Een gevolg hiervan is dat bedrijven meer aandacht lijken te besteden aan de beveiliging van systemen. Het *Office* leidt dit af uit een toegenomen verkoop van *encryption software* sinds de invoering van de meldplicht.

Een nadeel van de meldplicht is volgens het *Office of Privacy Protection* dat deze bedrijven ook verplicht te melden wanneer er feitelijk weinig aan de hand is. De meldplicht schrijft voor dat verlies van een laptop of het verkeerd bezorgen van post zo snel mogelijk wordt gemeld, terwijl het vaak een dag later is opgelost omdat de laptop wordt teruggebracht of de post alsnog juist wordt bezorgd.

[1] Website: www.oispp.ca.gov/consumer_privacy

9 Nevada

Wanneer ingegaan	1 januari 2006
Welke wet	SB. 347, Nev. Rev. Stat. 607A.010
Doel	Meldplicht onderdeel van een bredere wet die identiteitsfraude tegen moet gaan
Voor welke organisaties	*Data collectors:* overheidsorganisaties, bedrijven en andere organisaties die 'handle, collect, disseminate or otherwise deal with non-public personal information'
Welke soort gegevens	Niet-versleutelde, digitale persoonsgegevens
Wanneer melden	Wanneer (een reële mogelijkheid bestaat dat) een onbevoegd persoon persoonsgegevens heeft verworven en nadat is aangetoond dat (het redelijkerwijs mogelijk is dat) deze gegevens zijn misbruikt voor ongeautoriseerde doeleinden.
Aan wie melden	Getroffen personen; bij meer dan 1000 getroffenen, ook aan 'all consumer reporting agencies'
Handhaving	Attorney General of District Attorney als hij van mening is dat een organisatie zich niet aan de wet houdt.
Bijzonderheden	Wetgevende macht van Nevada vergadert slechts eens per twee jaar en heeft weinig capaciteit. Meldplicht daarom letterlijk gekopieerd uit federale wetgeving en wetgeving andere staten.

9.1 Aanleiding

De meldplicht in Nevada maakt deel uit van een wet die als doel heeft identiteitsfraude tegen te gaan. De onderliggende reden van de invoering van deze wet was een toename van identiteitsfraude in de staat. Er was geen informatie beschikbaar over het aantal veiligheidsinbreuken. Wel was bekend dat het aantal arrestaties voor ID-fraude gerelateerde misdrijven door politie en justitie steeds meer toenam. De invoering van de wet had daarnaast net als in Californië een persoonlijke oorzaak; één van de 'sponsors' was slachtoffer geworden van identiteitsfraude.

Mogelijke oorzaken hoog percentage identiteitsfraude Nevada

Nevada is een van de staten in de Verenigde Staten waar identiteitsfraude het vaakst voorkomt. De volgende oorzaken liggen hieraan mogelijk ten grondslag:

- Er zijn indicaties dat er een verband is tussen het hoge percentage gebruik illegale drug methamphetamine in Nevada en identiteitsfraude. Voor verslaafden zou computercriminaliteit een veilige manier zijn om aan geld te komen.
- Mogelijk speelt de aanwezigheid van Las Vegas ook een rol. De bevolking van deze stad is voortdurend in beweging, net als de omvangrijke geldstromen als gevolg van de toeristen- en gokindustrie van de stad. Voor criminelen is het makkelijk om hun activiteiten te verdoezelen door de vele geldtransacties in en uit banken.

Uit interviews komt naar voren dat invoering van de meldplicht niet op tegenstand is gestuit en dat er weinig aandacht is besteed, nadat deze was ingevoerd. De reden is waarschijnlijk omdat op federaal niveau al dergelijke wetgeving was ingevoerd. Volgens respondenten was het met name de federale meldplicht die organisaties motiveerde om veiligheidsinbreuken te gaan melden.

9.2 Vormgeving

De vormgeving van Nevada's meldplicht komt sterk overeen met wetgeving op federaal niveau en in Californië.

Doelgroep
De meldplicht is van toepassing op *alle data collectors*: overheidsorganisaties, opleidingsinstituten, financiële instellingen, bedrijven en elke andere organisatie die 'handle, collect, disseminate or otherwise deal with non-public personal information'. Data collectors zijn niet gebonden aan de meldplicht als zij vallen onder de Gramm-Leach-Bliley Act of zelf beleid hebben geïmplementeerd voor het melden van veiligheidsinbreuken.
Een brede doelgroep is volgens respondenten passend, omdat men ervaart dat grote, commerciële instellingen als kwetsbaar worden gezien door hackers en daarom vaak het doelwit zijn van hackpogingen (bijvoorbeeld TJX).

Soort gegevens
De meldplicht geldt voor niet-versleutelde, digitale persoonsgegevens. Omdat de wet als geheel ook van toepassing op papieren data, geldt de meldplicht volgens respondenten ook wanneer er toegang is verkregen tot papieren data. Persoonsgegevens worden hetzelfde gedefinieerd als in o.a. Californië.

Grondslag voor melding
Ook de grondslag is dezelfde als in Californië. Een data collector moet een veiligheidsinbreuk melden wanneer (een reële mogelijkheid bestaat dat) een onbevoegd persoon persoonsgegevens heeft verworven. Nevada verplicht de data collector om eerst onderzoek te doen om te bekijken of (het redelijkerwijs mogelijk is dat) deze gegevens zijn misbruikt voor ongeautoriseerde doeleinden. De data collector bepaalt zelf of melding nodig is.

Aan wie melden
Net als in Californië, moet de data collector de eigenaar van de persoonsgegevens, ofwel de getroffen burger of consument, zo snel mogelijk en zonder vertraging op de hoogte stellen van de veiligheidsinbreuk. De vorm en de procedure voor melding zijn ook hetzelfde als in Californië.

9.3 Handhaving en toezicht

Nevada kent geen onafhankelijke toezichthouder. De meldplicht wordt achteraf gehandhaafd door de Attorney General of de District Attorney. Wanneer hij van mening is dat een organisatie zich niet aan de wet houdt, kan hij een dwangbevel opleggen. De data collector zelf kan daarnaast via de rechtbank een schadevergoeding eisen van de degene die van de veiligheidsinbreuk heeft geprofiteerd.

Volgens respondenten kan een meldplicht weinig effectief worden gehandhaafd. Het is niet waarschijnlijk dat de Attorney General als eerste op de hoogte geraakt van een veiligheidsinbreuk of erachter komt dat een organisatie zich niet aan de meldplicht houdt. Dit is de consequentie van de neiging van organisaties om veiligheidsinbreuken intern te houden (zie verder: Evaluatie). Bovendien, als Justitie al op de hoogte is van een veiligheidsinbreuk, zit er voor de organisatie niets anders op dan ook de betrokkenen op de hoogte te stellen. Een dwangbevel is dan eigenlijk niet meer nodig.

9.4 Wettelijk kader

De meldplicht in Nevada maakt deel uit van een wet die als doel heeft identiteitsfraude tegen te gaan. Een belangrijke motivatie om een meldplicht op staatsniveau te implementeren, was om de Officier van Justitie en burgers in staat te procederen wanneer een veiligheidsinbreuk of identiteitsfraude binnen de grenzen van de staat plaatsvindt. In de praktijk wordt er nauwelijks op staatsniveau geprocedeerd wanneer een veiligheidsinbreuk plaatsvindt: het betreft meestal veiligheidsinbreuken bij grote organisaties die op nationaal niveau werkzaam zijn. Volgens respondenten is er de afgelopen tijd 1 keer een beroep gedaan op Nevada's meldplicht, toen een inbreuk plaatsvond bij de deelstaatoverheid zelf.

Consequenties bijzondere vergadercyclus wetgevende macht Nevada
Anders dan in veel andere staten, bevat de meldplicht geen elementen of eisen specifiek voor Nevada. De wetgevende macht heeft de tekst van de meldplicht vrij letterlijk overgenomen van wetten op federaal niveau en omliggende staten, komt uit interviews naar voren. De wetgevende macht van Nevada komt namelijk slechts eens per twee jaar bijeen en heeft weinig capaciteit om wetgeving voor te bereiden. Nieuwe wetten worden daarom vaak gebaseerd op wetgeving van andere staten.

Eisen aan encryptie
Nevada probeert ook via andere wegen organisaties te stimuleren hun data beter te beveiligen. Een ander statuut dat recentelijk is ingevoerd, vereist dat organisaties 'data in transit' beveiligen door encryptie. 'Data in transit' zijn gegevens die buiten de beveiligde omgeving van de organisatie worden vervoerd, op laptops of memoriesticks. Organisaties die hun data op deze manier beveiligen, zijn in mindere mate aansprakelijk wanneer er een veiligheidsinbreuk plaatsvindt. Zo probeert Nevada organisaties te motiveren hun data beter te beschermen. Bij voorkeur van Nevada's Technological Crime Advisory Board worden in de toekomst ook eisen gesteld aan het versleutelen van 'data in rest'.

9.5 Evaluatie en lessen

De waarde van een meldplicht is volgens respondenten dat organisaties worden gemotiveerd om meer aandacht aan beveiliging te besteden; ook worden burgers bewuster van het belang van de bescherming van persoonsgegevens.

Het cruciale punt van een meldplicht is om de *'internal risk analysis within companies'* te beïnvloeden. Om imago- en financiële schade te voorkomen, zijn organisaties namelijk geneigd om te 'undernotify'. Dit baseren respondenten op ervaringen van mensen die bij discussies over het al dan niet melden van een inbreuk binnen een bedrijf aanwezig zijn geweest. Organisaties nemen met liever het risico de kleinere veiligheidsinbreuken niet te melden, waarvan het niet duidelijk is of überhaupt sprake was van een inbreuk. Deze inbreuken zijn makkelijker te verbergen en zouden alleen onder de aandacht komen wanneer de organisatie deze zelf meldt.

De meldplicht moet organisaties een afdoende stimulans bieden om veiligheidsinbreuken wel te melden. De vraag is echter *hoe* de interne risicoanalyse van een organisatie het meest effectief kan worden beïnvloed. Het is volgens respondenten de vraag of de huidige meldplicht in Nevada voldoende prikkels geeft. Een klokkenluider zou mogelijk een additionele stimulans zijn voor organisaties.

10 Noorwegen

Wat	Meldplicht
Wanneer	14 april 2000
Wet	Personal Data Act: Act of 14 april 2000 No. 31 relating to the processing of personal data, Chapter II, Section 2-6
Doel	Verzamelen van informatie over veiligheidsinbreuken om Datatilsynet in staat te stellen organisaties te helpen de 'normale situatie' te herstellen door verbetering van veiligheidsmaatregelen
Voor welke organisaties	Alle data controllers (organisaties die persoonsgegevens be- en verwerken) die zijn gevestigd in Noorwegen en data controllers buiten de EEG die gebruik maken van *equipment* in Noorwegen
Welke gegevens	Gevoelige en vertrouwelijke persoonsgegevens
Wanneer melden	Organisaties dienen melding te maken aan de toezichthouder indien een 'discrepantie' leidt tot de onbevoegde openbaarmaking van persoonsgegevens.
Aan wie melden	De nationale toezichthouder: Datatilsynet
Handhaving	Datatilsynet: inspectie, indienen formele klacht over een veiligheidsinbreuk bij Justitie, publicatie, advies
Bijzonderheden	Noorwegen tot op heden enige land in Europa met een meldplicht

10.1 Aanleiding en discussie

De aanleiding voor het invoeren van de meldplicht in privacy wetgeving was de behoefte van de nationale toezichthouder, Datatilsynet, aan meer informatie over veiligheidsinbreuken bij organisaties[1]. Met deze informatie kan Datatilsynet organisaties helpen de 'normale situatie' te herstellen door verbetering van veiligheidsmaatregelen. Met een 'normale situatie' wordt een situatie bedoeld waarin geen veiligheidsinbreuken meer plaatsvinden.

Voor zover bekend is er geen discussie geweest over de invoering en de inhoud van de meldplicht. Uit het interview komt naar voren dat de behoefte aan een meldplicht er altijd is geweest. Gegevens over het aantal veiligheidsinbreuken waren niet bekend en zijn dat nu nog niet; Datatilsynet richt zich op cases en houdt het aantal inbreuken niet bij.

[1] Datatilsynet is opgericht in 1980 en valt formeel onder het Noorse ministerie van Werkgelegenheid en Binnenlandsbestuur[1].

10.2 Inhoud meldplicht

De inhoud van de meldplicht is voor een deel gebaseerd op de ISO 27000 standaard betreffende informatiemanagement en –beveiliging[1]. Deze set met richtlijnen beschrijft een model voor het opzetten, uitvoeren, monitoren en verbeteren van informatiebeveiligingssystemen en schrijft de eisen voor waaraan organisaties moeten voldoen om een certificaat te krijgen.

Het doel van de Personal Data Act is "to protect natural persons from violation of their right to privacy through the processing of personal data."

Wettelijk kader

De meldplicht is opgenomen in de Personal Data Act, die in werking trad op 14 april 2000. De voorganger van deze wet stamt uit 1978. Hoewel Noorwegen niet tot de EU behoort, implementeerde de overheid met de nieuwe Personal Data Act EU Directive 95/46/EC in de Noorse wetgeving.

Naast een meldplicht in geval van gegevensverlies, verplichten Secties 31-32 van de Act organisaties melding te maken Datatilsynet, de nationale toezichthouder verantwoordelijk voor de handhaving van de Personal Data Act, voordat zij persoonsgegevens beginnen te verwerken. In sommige gevallen moet de organisatie eerst een vergunning aanvragen om persoonsgegevens te mogen verwerken. Dit geldt voor gevoelige gegevens en gegevens die worden verwerkt door de verzekerings-, bancaire en telecomsector[2]. Datatilsynet beheert een openbaar register met daarin de informatie over organisaties met een vergunning.

Doelgroep

De Personal Data Act geldt voor alle data controllers die zijn gevestigd in Noorwegen en data controllers van buiten de Europese economische zone (de EU plus Noorwegen, Ysland and Liechtenstein), die gebruik maken van *equipment* in Noorwegen[3]. Kortom, de meldplicht geldt voor zowel overheidsorganisaties als de private sector en heeft zo een brede scope.

Welke gegevens?

De Personal Data Act geldt voor zowel niet-digitale als digitale registers. De wet is van toepassing op persoonsgegevens en gevoelige en vertrouwelijke persoonsgegevens. De meldplicht geldt voor de laatste categorie. Onder gevoelige persoonsgegevens verstaat de wet gegevens die zijn gerelateerd aan:

- raciale of etnische origine, politieke, filosofische of religieuze overtuigingen;
- het feit dat een persoon is verdacht van een misdrijf of daarvoor is aangeklaagd of veroordeeld;
- gezondheid;
- seksleven;
- lidmaatschap van een vakbond[4].

Uit de combinatie van afzonderlijke gegevens van niet-gevoelige aard kan immers een vertrouwelijk, persoonlijk profiel ontstaan.

[1] Website: www.27000.org
[2] Personal Data Act: Act of 14 april 2000 No. 31 relating to the processing of personal data, Chapter 7
[3] Een uitzondering wordt gemaakt voor data controllers die deze equipment om data via Noorwegen te verplaatsen.
[4] Personal Data Act: Act of 14 april 2000 No. 31 relating to the processing of personal data, Chapter I, Section 2, 8 a t/m e

Uit het interview blijkt dat vertrouwelijke persoonsgegevens lastiger zijn te definiëren. Een voorbeeld is de discussie over de vertrouwelijkheid van IP-adressen. Datatilsynet beschouwt IP-adressen als vertrouwelijke informatie, terwijl het bedrijfsleven dat niet zo ziet en het verlies van IP-adressen vaak niet meldt.

Grondslag voor melding
Organisaties dienen melding te maken aan de toezichthouder indien een 'discrepantie' leidt tot de onbevoegde openbaarmaking van persoonsgegevens.

Aan wie melden en hoe?
De organisatie moet het gegevensverlies melden aan consumenten en Datatilsynet. In de praktijk wordt Datatilsynet geacht volledig onafhankelijk van de overheid en de private sector te functioneren. Er is formeel geen exacte deadline vastgesteld voor de melding, maar het is van belang dat een veiligheidsinbreuk zo snel mogelijk wordt gemeld, het liefst dezelfde dag nog. De melding aan Datatilsynet kan zowel schriftelijk als per e-mail geschieden. Het is niet helder wat de richtlijn is om consumenten op de hoogte te stellen; uit het interview komt naar voren dat zij 'in the best way' moeten worden geïnformeerd.

10.3 Handhaving en naleving

Datatilsynet is verantwoordelijk voor de handhaving van de Personal Data Act en daarmee de meldplicht. De toezichthouder kan hiertoe inspecties uitvoeren en organisaties verplichten hun beveiliging te verbeteren. De toezichthouder beoordeelt per case welke acties hij zal ondernemen. In geval van een zeer ernstige veiligheidsinbreuk of wanneer inbreuken meer dan eens plaatsvinden, bezoekt Datatilsynet de organisatie om de databeveiliging te inspecteren. De nadruk van dit bezoek ligt op advies over de verbetering van veiligheidsmaatregelen.

Publicatie
Het inspectierapport wordt gepubliceerd op de website van de toezichthouder. Voor publicatie mag de data controller het rapport inzien voor correctie. Zolang de data controller nog niet heeft gereageerd, wacht Datatilsynet met de publicatie. Voorzover bekend kan de organisatie publicatie niet tegenhouden, maar biedt de mogelijkheid tot inzage organisaties wel een kans om publicatie te vertragen.

Geen boetebevoegdheid, wel klacht
Datatilsynet heeft geen boetebevoegdheid, maar kan wel een formele klacht indienen bij Justitie over een veiligheidsinbreuk zoals in het geval van het verlies van 20.000 *social security* nummers. Hierop volgt mogelijk een justitieel onderzoek en eventueel een aanklacht. Schending van de Personal Data Act kan leiden tot een boete, een gevangenisstraf of het betalen van schadevergoeding aan getroffen consumenten.

Voorkeur voor goede verstandhouding
Datatilsynet hecht niet veel waarde aan sanctioneren door boetes. Het beleid van Datatilsynet is meer gericht op het geven van advies en het onderhouden van een goede verstandhouding met organisaties dan straffen. Datatilsynet is van mening dat het belangrijk is om data controllers door middel van discussie ervan te overtuigen dat de beveiliging van persoonsgegevens belangrijk is. Daarnaast wil Datatilsynet data controllers niet ontmoedigen veiligheidsinbreuken te melden en de toezichthouder om advies te vragen over beveiliging.

Uit de praktijk volgt een ander bezwaar tegen boetes: organisaties blijken vaak ongevoelig voor boetes. Veiligheidsinbreuken komen vaak onder de aandacht van de toezichthouder via de media of een inspectie. Data controllers zijn banger voor de imagoschade die de publicatie van het inspectierapport tot gevolg heeft. Organisaties proberen vaak te voorkomen dat Datatilsynet de veiligheidsinbreuk publiceert.

10.4 Evaluatie

Datatilsynet beschouwt de meldplicht als belangrijke wetgeving. Datatilsynet vindt het positief dat er nu wetgeving op Europees niveau wordt ontwikkeld; landen kunnen van elkaars ervaringen leren.
De vraag is hoe effectief de Noorse meldplicht is. Het hoofddoel van de meldplicht, het verbeteren van de beveiliging van persoonsgegevens door organisaties, is een langdurig proces en is nog niet bereikt. Uit een recente survey door Datatilsynet bleek dat veel bedrijven niet bewust met de beveiliging van persoonsgegevens bezig zijn; ook zijn bedrijven vaak onvoldoende op de hoogte van de inhoud van de Personal Data Act. Hoewel organisaties volgens Datatilsynet nu wel op de hoogte zijn van de meldplicht, worden veel veiligheidsinbreuken volgens respondenten niet gemeld.

Case-studies:
landen met vrijwillige melding

- Canada
- Australië

11 Canada

Wat	Vrijwillige melding van veiligheidsinbreuken voor private sector; voorstellen voor meldplicht voor bedrijven *en* overheidsorganisaties
Wanneer ingegaan	Vrijwillige melding: niet bekend Meldplicht: niet bekend, voorstel d.d. 11 april 2008
Welke wet	Vrijwillige melding, vormgegeven in gids; meldplicht zou in Personal Information Protection and Electronic Documents Act (PIPEDA) en Privacy Act moeten worden opgenomen.
Doel	1) bedrijven meer stimuleren om veiligheidsmaatregelen te verbeteren; 2) burgers geruststellen; 3) verkrijgen van meer informatie over veiligheidsinbreuken, zodat Privacy Commissioner organisaties beter kan begeleiden.
Voor welke organisaties	Private sector en overheidsorganisaties
Welke soort gegevens	Persoonsgegevens; opgeslagen op *alle* soorten media, inclusief papier, bandopnamen en video.
Wanneer melden	Voorstel meldplicht PIPEDA bevat tweeledige grondslag: melden wanneer sprake is van (1) 'material breach' en (2) wanneer sprake is van 'significant harm' voor burgers
Aan wie melden	Stap 1: 'Material breach' melden aan toezichthouder; Stap 2: 'Significant harm' melden aan getroffen burgers.
Handhaving	Toezichthouder: Office of the Privacy Commissioner. Behalve bevoegdheid om audits uit te voeren, aanbevelingen uit te brengen en naming & shaming, momenteel geen handhavingsbevoegdheden.
Bijzonderheden	Vrijwillige melding levert volgens OPC te weinig informatie over veiligheidsinbreuken op.

11.1 Aanleiding, discussie en doelstellingen

Op dit moment kent Canada nog geen meldplicht. Er geldt een aantal jaren een vrijwillige melding voor de private sector, welke de Privacy Commissioner in 2008 heeft vormgegeven in een gids[1]. Ook overheidsorganisaties kunnen veiligheidsinbreuken vrijwillig melden, maar dit is niet formaliseerd. Een aantal provincies kent ook een vrijwillige melding voor de private sector, namelijk Quebec, Alberta, British Columbia; Ontario heeft een vrijwillige melding opgenomen voor de gezondheidszorg. De Canadese overheid bracht in juni 2008 een voorstel uit voor een meldplicht voor de private sector en overheidsorganisaties[2]. Dit voorstel is het resultaat van intensief overleg met stakeholders.

Discussie
De Privacy Commissioner geeft de voorkeur aan een meldplicht, omdat de vrijwillige melding onvoldoende informatie over het aantal en de aard van veiligheidsinbreuken oplevert.

[1] Draft Voluntary Information Security Breach Notification Guide, April 2008: http://www.privacy.gov.au/publications/breach_0408.html#Voluntary
[2] Industry Canada, A model for data breach reporting and notification under PIPEDA (June 2008)

Een aantal bedrijven is van mening dat een meldplicht niet nodig is, omdat de vrijwillige melding volgens hen *wel* goed werkt. Grote bedrijven zijn volgens respondenten bereid zich achter de invoering van een meldplicht te scharen, op voorwaarde dat de lat voor melding hoog wordt gelegd.

Doelstellingen
Met een meldplicht wil de Canadese overheid drie doelen bereiken: (1) bedrijven meer stimuleren om veiligheidsmaatregelen te verbeteren; (2) door verplichte melding burgers geruststellen; (3) verkrijgen van meer informatie over veiligheidsinbreuken, zodat de Privacy Commissioner organisaties beter kan begeleiden.

Groot en klein
De Privacy Commissioner ziet vooral kansen om via een meldplicht kleinere en middelgrote bedrijven beter te begeleiden bij het verbeteren van hun beveiliging. Grote organisaties, banken en vliegtuigmaatschappijen dragen zelf zorg voor deze beveiliging, stellen respondenten. Zij zouden via een meldplicht beter kunnen worden gewezen op hun verantwoordelijkheden als het gaat om de bescherming van persoonsgegevens.

11.2 Vormgeving voorgestelde meldplicht private sector

Doelgroep
In Canada is voorgesteld om een meldplicht in te stellen voor zowel de private als de publieke sector. Deze paragraaf richt zich op het voorstel voor de private sector.

Soort gegevens
Net als in Australië en anders dan in de Verenigde Staten, is Canada van mening dat een meldplicht niet alleen moet gelden voor digitale persoonsgegevens, maar voor *elk* medium dat persoonsgegevens draagt. De meldplicht is van toepassing op *alle* soorten media, inclusief papier, bandopnamen en video.

Grondslag voor melding en melden aan wie
De voorgestelde grondslag voor melding is tweeledig en vertoont in die zin overeenkomsten met het Europese model. De lat voor melding is opzettelijk hoog gelegd, omdat het bedrijfsleven niet bereid is zich achter een meldplicht te scharen die hen verplicht *alle* veiligheidsinbreuken te melden. De grondslag voor melding aan de toezichthouder is ‘material breaches’ (1); de grondslag voor melding aan consumenten is ‘significant harm’ (2)[1].

Material breaches: melding aan toezichthouder
Bedrijven hoeven alleen ‘material breaches’ te melden aan de toezichthouder. Om te bepalen of er sprake is van een ‘material breach’ stelt Industry Canada (het departement dat verantwoordelijk is voor de herziening van de privacy wetgeving) drie criteria voor waar bedrijven rekening mee zouden moeten houden:
- Gevoeligheid van de gecompromitteerde informatie;
- Het aantal personen dat wordt geschaad door de inbreuk;

[1] Industry Canada, A model for data breach reporting and notification under PIPEDA (June 2008)

- Is er sprake van een ‘systemic root cause’?

De laatste twee criteria vloeien voort uit de gehanteerde definitie van een ‘veiligheidsinbreuk’. De nadruk ligt hierbij op veiligheidsinbreuken waarbij de *beveiligingsmaatregelen* van een bedrijf, opzettelijk of onopzettelijk, worden doorbroken. Om deze reden heeft Industry Canada ook het criterium van een aantal geschaadde personen opgenomen. Het is namelijk niet de bedoeling van de toezichthouder wordt geïnformeerd over elke brief die kwijtraakt.

Definitie veiligheidsinbreuk

“Data breach” means an incident involving loss of, unauthorized access to, or disclosure of, personal information as a result of a breach of an organization’s security safeguards pursuant to Principle 7 of Schedule 1 of PIPEDA.’

Bron: Industry Canada, A model for data breach reporting and notification under PIPEDA (June 2008)

Significant harm: melding aan consument

Als de toezichthouder van mening is dat er een hoog risico op significante schade is voor de betrokken consumenten, moet het bedrijf de betrokken personen alsnog op de hoogte stellen. Dit geldt ook als het bedrijf in eerste instantie zelf dit risico constateert. ‘Schade’ wordt hier breed gedefinieerd. Anders dan in veel Amerikaanse deelstaten, waar de nadruk vaak op financiële schade ligt, houdt het Canadese model ook rekening met reputatieschade, medische gevolgen of schade gerelateerd aan het werk van de consument. Om te bepalen of het risico op schade hoog is, zijn de volgende criteria opgesteld:

- Gevoeligheid van de gecompromitteerde informatie;
- Waarschijnlijkheid dat de informatie wordt misbruikt;
- De significantie van de schade: financieel, identiteitsfraude, reputatieschade, vernedering, medische schade etc.

11.3 Handhaving en toezicht

De toezichthouder heeft momenteel geen sterke handhavingsbevoegdheden. Zij kan momenteel wel audits uitvoeren, maar deze resulteren alleen in aanbevelingen aan de organisatie over de verbetering van de beveiliging van persoonsgegevens. De Privacy Commissioner heeft geen boetebevoegdheid en kan navolging van de aanbevelingen niet afdwingen; daarvoor moet zij naar de rechter. Wel past de toezichthouder naming & shaming toe door informatie over veiligheidsinbreuken bij organisaties te publiceren. Industry Canada heeft voorgesteld dat de toezichthouder in geval van de meldplicht veiligheidsinbreuken ook in een rapport aan het Parlement zou moeten melden. Volgens respondenten zijn er geen plannen om de huidige bevoegdheden nog verder uit te breiden onder de meldplicht.

Wel is het mogelijk dat de regering beslist om de capaciteit van de toezichthouder uit te breiden, zeggen respondenten. Momenteel heeft de toezichthouder te weinig mankracht om een meldplicht te kunnen handhaven; de vrijwillige melding wordt nu behandeld door 1 persoon (notification officer, NOF).

11.4 Wettelijk kader

De vrijwillige melding is vormgegeven in een gids. Een meldplicht zou moeten worden opgenomen in de privacy wetgeving. In Canada geldt voor de private en publieke sector andere wetgeving. De meldplicht voor de private sector zou in de privacy wetgeving die voor het bedrijfsleven geldt moeten worden opgenomen, de Personal Information Protection and Electronic Documents Act (PIPEDA); een meldplicht voor de publieke sector in de Privacy Act, de privacy wetgeving voor overheidsorganisaties.

12 Australië

Wat	Vrijwillige melding veiligheidsinbreuk als voorloper meldplicht in herziene privacy wetgeving
Wanneer	Augustus 2008, meldplicht mogelijk over 2 jaar
Wet	Gids uitgebracht door Office of the Privacy Commissioner: Guide to handling personal information security breaches
Doel	Het begeleiden van organisaties bij het omgaan met een veiligheidsinbreuk; Het verzamelen van *best practices* en adviezen betreffende vrijwillige melding veiligheidsinbreuken ter voorbereiding van meldplicht onder herziene privacy wetgeving.
Voor welke organisaties	Bedrijven en overheidsorganisaties
Welke gegevens	Beveiligde (encrypted) persoonsgegevens in elke vorm
Wanneer	Wanneer het verlies, onbevoegde toegang, gebruik, openbaarmaking, kopiëren of aanpassen van persoonsgegevens mogelijk leidt tot ernstige schade voor betrokkenen
Aan wie melden	Privacy Commissioner en individuen
Handhaving	Onderzoek, audits, eis (financiële) compensatie getroffenen, geen boetebevoegdheid. Mogelijk wel boetebevoegdheid onder herziene privacy wetgeving
Bijzonderheden	Australië, na Canada en Nieuw Zeeland, derde land ter wereld met een vrijwillige meldplicht.

12.1 Aanleiding

De vrijwillige melding van gegevensverlies in Australië is niet getriggered door een incident. Australië kent weinig tot geen grote dataschandalen. Mede dankzij de Britse en Amerikaanse dataschandalen wordt identiteitsfraude wel steeds belangrijker gevonden door het publiek; de meeste klachten die Privacy Commissioner in 2007/08 ontving, gingen over dit onderwerp.
In privacy wetgeving, die op dit moment wordt herzien en naar verwachting over 2 jaar ingaat, zal een meldplicht worden opgenomen. De Privacy Commissioner heeft afgelopen zomer een gids geïntroduceerd bij wijze van voorbereiding op deze meldplicht[1]. De gids is ontwikkeld om bedrijven en organisaties te helpen bij het omgaan met veiligheidsinbreuken, in reactie op verzoeken om advies en bij wijze van erkenning van de internationale trends op dit gebied. De Australische gids is gebaseerd op de vrijwillige meldplichten in Canada en Nieuw Zeeland.

[1] Office of the Privacy Commissioner: Guide to handling personal information security breaches.

12.2 Discussie

De meldplicht wordt gaandeweg ontwikkeld in samenspraak met verschillende stakeholders. Het concept van de gids is in April 2008 verspreid onder bedrijven, NGO's en (semi-) overheidsorganisaties. Het OPC ontving 75 reacties, de federale overheid zal ook nog reageren. De reacties bevatten volgens de Privacy Commissioner goede suggesties voor verdere ontwikkeling van de gids. Ook bleek uit de reacties dat een meldplicht breed wordt gedragen.

Omdat identiteitsfraude een steeds belangrijker onderwerp wordt, vindt men het tijd om iets te ondernemen. De algemene opinie is dat burgers het recht hebben om te weten dat hun data in gevaar zijn; de gids wordt gezien als een manier om de controle van burgers over hun gegevens te vergroten. Bedrijven willen hun klanten niet kwijtraken en zijn bereid maatregelen te nemen om de bescherming van de privacy van consumenten te verbeteren.

Sommige bedrijven staan negatief tegenover een meldplicht, omdat zij verwachten dat dit hoge kosten met zich meebrengt.

12.3 Inhoud van de gids en voorstel meldplicht

De gids adviseert bedrijven en overheidsorganisaties over hoe het beste kan worden omgegaan met veiligheidsinbreuken. Een gedetailleerd stappenplan moet organisaties helpen bij het maken van de beslissing of een veiligheidsinbreuk ernstig genoeg is om te melden. Het OPC adviseert vier stappen die een organisatie kan nemen in geval van een veiligheidsinbreuk:

STAP 1: beperk (*contain*) de inbreuk en voer een voorbereidende analyse uit

STAP 2: evalueer de risico's die gepaard gaan met de inbreuk

STAP 3: overweeg melding

STAP 4: voorkom inbreuken in de toekomst

Bij elke stap beschrijft de OPC de overwegingen waar de organisatie rekening mee moet houden om te komen tot een bepaalde keuze. Ook bevat de gids voorbeelden om bepaalde keuzes te illustreren.

Doelgroep
De meldplicht zou moeten gelden voor overheidsorganisaties en bedrijven.

Soort gegevens
Het OPC en de ALRC zijn van mening dat een meldplicht niet beperkt moet zijn tot *computerized* of financiële gegevens, wat in de Verenigde Staten vaak het geval is. De meldplicht moet zo breed mogelijk zijn. Het is echter niet nodig om beveiligde data te melden.

De ALRC adviseert om de meldplicht van toepassing te laten zijn op 'specifieke persoonsgegevens', een combinatie van persoonsgegevens en gevoelige informatie als gedefinieerd

onder de huidige Privacy Act. Specifieke persoonsgegevens moeten in 'goed vertrouwen' zijn verkregen en betreffen naam en adres in combinatie met:

- Rijbewijs of ander bewijs van geboortedatum
- *Medicare* nummer of een ander uniek ideniticatienummer
- Rekening-, creditcard of pinpasnummers samen met een paswoord of toegangscode
- Gevoelige informatie, ofwel informatie over raciale of etnische origine, politieke of religieuze overtuigingen; het feit dat een persoon is verdacht van een misdrijf of daarvoor is aangeklaagd of veroordeeld; gezondheid; seksleven; lidmaatschap van een vakbond[1].

Grondslag voor melding

Als grondslag voor melding stellen ALRC en OPC 'real risk of serious harm' voor. Het risico is niet beperkt tot identiteitsfraude of diefstal, maar omvat ook discriminatie als gevolg van diefstal van gevoelige medische gegevens. Schade omvat fysieke en financiële schade, imagoschade en schade voor de werkgelegenheid van de getroffene.

Melding moet geschieden in elke situatie wanneer het verlies, onbevoegde toegang, gebruik, openbaarmaking, kopiëren of aanpassen van persoonsgegevens volgens de organisatie mogelijk leidt tot ernstige schade voor betrokkenen. Om te bepalen of melding nodig is, kan de organisatie de 4 stappen van de OPC doorlopen en zo rekening met de aard van de persoonsgegevens, oorzaak en reikwijdte van de inbreuk, wie wordt gedupeerd en wat de mogelijke schade is. De ALRC acht het van belang dat de beslissing om te melden wordt genomen samen met de Privacy Commissioner.

Privacy Commissioner krijgt 'oversight power', zodat de beslissing om te melden in consultatie met de OPC wordt genomen.

Deze grondslag biedt volgens de ALRC en OPC een hogere drempel voor melding dan bijvoorbeeld 'unauthorized acquisition', omdat de organisatie rekening moet houden met meerdere factoren. Een hoge drempel is nodig om een overvloed van meldingen aan burgers te voorkomen.

Een minimum aantal gedupeerden of verloren gegevens is niet overwogen; een inbreuk kan immers voor een individu ook veel schade opleveren.

Aan wie melden en hoe?

Organisaties en getroffen individuen. De ALRC en de OPC willen niet voorschrijven welke vorm de melding moet hebben, omdat een organisatie dat volgens hen het beste zelf kan beslissen. De gids stelt wel dat de directe melding aan de getroffenen de voorkeur verdient boven een indirecte melding via de media.
De gids adviseert ook om het volgende in een melding op te nemen: omschrijving incident, aard gegevens, reactie organisatie op de inbreuk, hulp aan de getroffenen, contactinformatie, of de inbreuk is gemeld aan de OPC, juridische implicaties en waar de getroffene een klacht kan indienen[2].

[1] PRIVACY ACT 1988 - SECT 6.
[2] OPC Breach Guide: What should be included in the notification? Pag 25.

12.4 Handhaving

De Privacy Commissioner is op dit moment verantwoordelijk voor de handhaving van de privacy wetgeving, en daarmee in de toekomst van de meldplicht. Op dit moment geeft de OPC alleen advies aan organisaties over het omgaan met een veiligheidsinbreuk. Wanneer een burger een klacht indient over gegevensverlies, is de OPC wel bevoegd om onderzoek uit te voeren bij de betreffende organisatie. Daarnaast kan de OPC zelf een onderzoek initiëren, audits uitvoeren en (financiële) compensatie voor getroffenen eisen. De rechter ziet toe op de naleving van de besluiten van de Commissioner. De OPC heeft momenteel echter niet genoeg mankracht om deze audits routinematig uit te voeren. De OPC verwacht dat haar middelen zullen worden uitgebreid als de meldplicht wordt geïmplementeerd.

Publicatie geen beleid
Het openbaar maken van veiligheidsinbreuken lijkt geen beleid te zijn van de OPC. Het is mogelijk dat hij in sommige gevallen onderzoeken wel publiceert, staat in de gids. Verder zou de Commissioner de verantwoordelijke minister op de hoogte kunnen stellen van het feit dat een organisatie zich niet aan de privacy wetgeving houdt.

Boetebevoegdheid in de toekomst
De OPC heeft nu geen boetebevoegdheid. De Commissioner kan van een organisatie eisen om een gedupeerde financieel te compenseren, maar kan dit niet zelf afdwingen. De ALRC adviseert om de OPC wel een boetebevoegdheid te geven zodra de meldplicht wordt geïmplementeerd[1]. Volgens de ALRC is een boete een stimulans voor organisaties om:

- melding te maken van veiligheidsinbreuken
- de OPC te raadplegen over het al dan niet melden van een veiligheidsinbreuk
- werknemers afdoende te instrueren over de beveiliging van persoonsgegevens

12.5 Wettelijk kader

In welke wet?
De meldplicht zal worden opgenomen in herziene privacy wetgeving, de Privacy Act, die stamt uit 1988 en was gebaseerd op OECD wetgeving. In 2005 verzocht het Parlement, op initiatief van de Privacy Commissioner, de *Law Reform Commission* (ALRC) advies uit te brengen over herziening. In Hoofdstuk 51 van het omvangrijke rapport dat de ALRC uitbracht, wordt de opname van een meldplicht aanbevolen[2]. De OPC heeft de criteria die de ALRC voorstelt overgenomen in de gids, *Guide to handling personal information security breaches.*

Door alle technologische ontwikkelingen was het volgens de PC nodig om te onderzoeken of de Privacy Act uit 1988 nog relevant was.

[1] http://www.austlii.edu.au/au/other/alrc/publications/reports/108/51.html#Heading51
[2] http://www.austlii.edu.au/au/other/alrc/publications/reports/108/51.html#Heading51

Case-studies:
discussie over mogelijke invoering meldplicht

- Europese Unie
- Duitsland
- Verenigd Koninkrijk

13 Europese Unie

Wat	Voorstellen en discussie meldplicht voor telecomsector
Ingangsdatum	Mogelijk lente 2009
Wet	Meldplicht zal worden opgenomen richtlijn breed pakket telecomwetgeving: - Directive 2002/58/EC of the European Parliament and the Council of 7 May 2002 on universal service and users' rights relating to electronic communications networks and services
Doel	Verbetering van *personal data privacy* in de telecomsector in de Europese Unie
Voor welke organisaties	Aanbieders van openbare, elektronische communicatiediensten (telecombedrijven en ISP's) *(*EC) of alle diensten van de informatiemaatschappij (EP)
Welke gegevens	(niet-versleutelde) persoonsgegevens
Grondslag voor melding	1. alle veiligheidsinbreuken 2. in geval van *imminent and direct danger* voor de gebruikers
Aan wie melden	Nationale toezichthouder en alle betrokkenen
Handhaving	Providers verplicht tot jaarlijkse rapportage veiligheidsinbreuken aan nationale toezichthouder en getroffen gebruikers. Toezichthouder kan op basis van dit rapport provider alsnog verplichten tot melding.
Bijzonderheden	Aantal definities momenteel nog onderwerp van discussie, zoals de reikwijdte van de meldplicht en de definitie van 'alle veiligheidsinbreuken'. Europese Raad van Ministers vormt op 27 november 2008 een mening over Richtlijn 2002/58/EC, waarna het Europees Parlement voor de laatste keer over het voorstel stemt.

13.1 Achtergrond introductie meldplicht

Op Europees niveau wordt reeds enige tijd gewerkt aan een meldplicht in geval van gegevensverlies in het kader van de hervorming van de Europese telecomwetgeving. Het pakket telecomwetgeving wordt teruggebracht naar vijf telecommunicatierichtlijnen. De meldplicht wordt opgenomen in een van deze 5 richtlijnen, 2002/58/EU: deze richtlijn betreft het verwerken van persoonsgegevens en de bescherming van privacy in de elektronische communicatie sector[1].

Als redenen voor de introductie van de meldplicht noemen respondenten een verhoogd bewustzijn bij burgers van identiteitsfraude (incidenten Verenigd Koninkrijk, Deutsche Telecom in Duitsland), de invoering van veiligheidsmaatregelen door de OECD in 2002 en de invoering van meldplicht in de Verenigde Staten. Daarnaast ontbrak in Artikel 4 van Directive 96/45/EC, dat gaat over het risicomanagement van databeheer, tot op heden een meldplicht.

[1] Directive 2002/58/EC of the European Parliament and the Council of 7 May 2002 on universal service and users' rights relating to electronic communications networks and services

Aanleiding en doel herziening

De aanleiding voor de wijziging van richtlijn 2002/58/EU is de hervorming van de telecommunicatiesector teneinde de Europese interne telecommunicatiemarkt te voltooien. In 2002 is besloten tot deze hervorming[1]. Het doel van de herziening van o.a. richtlijn 2002/58/EU is:

"(…) to enhance the protection of personal data and the privacy of individuals in the electronic communications sector, in particular, by strengthening security-related provisions and enforcement mechanisms."[2]

In november 2007 bracht de Europese Commissie, na twee overlegronden met stakeholders en een *impact assessment,* twee voorstellen uit voor de herziening van het Europese telecompakket. Onderdeel van een van de voorstellen was de introductie van een meldplicht in geval van gegevensverlies in richtlijn 2002/58/EC. Sinds november vorig jaar hebben verschillende partijen gereageerd op dit voorstel, zoals de *European Data Protection Supervisor* (EDPS), en de Art. 29 Working Party, ofwel de *Working Party on the Protection of Individuals with regard to the Processing of Personal Data*. In september 2008 heeft het Europees Parlement gestemd over een voorstel voor herziening van het telecompakket en daarmee ook over de inhoud van de meldplicht[3].

Op het moment dat dit onderzoek wordt uitgevoerd, is een aantal aspecten van de meldplicht nog onderwerp van discussie. De voorstellen van de Commissie en het Parlement verschillen van elkaar wat betreft de reikwijdte en de grondslag van melding. Het Europees Parlement en de Europese Commissie verschillen van mening over de reikwijdte van de meldplicht. De Europese Commissie wil de meldplicht beperken tot de organisaties die vallen onder de Europese telecomwetgeving, ofwel telecombedrijven en internet service providers (ISP's). Het Europees Parlement heeft de voorkeur voor een meldplicht die verder gaat en voor *alle* diensten van de informatiemaatschappij geldt.

13.2 Voorstel Europese Commissie (November 2007)

Met de wijziging van richtlijn 2002/58/EU introduceert de Commissie een verplichte melding van veiligheidsinbreuken die resulteren in het verlies of gevaar lopen van persoonsgegevens van gebruikers of abonnees. Providers moeten de veiligheidsinbreuk zo snel mogelijk melden aan gebruikers. Daarbij moeten zij de gebruikers adviseren over voorzorgsmaatregelen om identiteitsfraude te voorkomen of te beperken. Ook moet een melding informatie bevatten over de maatregelen die de provider zelf neemt om de veiligheidsinbreuk aan te pakken.

[1] Advies Europees Economisch en Sociaal Comité, p. 4
[2] [Opinie WP 150, p. 2]
[3] Voorstel Europees Parlement 22 september 2008 over meldplicht: Amendementen 26, 31, 32, 183

Beperkte reikwijdte
De meldplicht die de Europese Commissie voorstelt, geldt voor *providers of publicly available electronic communication network services*[1]. Onder deze definitie vallen de internet service providers (ISP's), maar bijvoorbeeld niet internetbankieren, Hyves of de databases van overheidsorganisaties. Papieren data maakt ook geen deel uit van deze definitie.

Grotere rol nationale toezichthouder
De Commissie kent een grotere rol toe aan de nationale toezichthouders. Zij zouden over de nodige middelen moeten beschikken om de belangen van burgers te waarborgen als het gaat om de bescherming van hun gegevens en privacy. Toezichthouders zouden daartoe informatie moeten hebben over veiligheidsinbreuken die hebben geleid tot het verlies of gevaar lopen van persoonsgegevens.

Met *publicly available networks* worden *openbare netwerken* bedoeld; voor iedereen toegankelijk.

Belang context inbreuk
Ook wijst de Commissie op het belang van het beperken van de waarschijnlijkheid dat een veiligheidsinbreuk leidt tot identiteitsfraude. De Commissie stelt dat bij verdere uitwerking van de meldplicht voldoende aandacht wordt geschonken aan de omstandigheden waarin de veiligheidsinbreuk heeft kunnen plaatsvinden, zoals de vraag of de persoonsgegevens zijn beveiligd (*encrypted*).

13.3 Reactie EDPS en Art. 29 Working Party (April/Mei 2008)

Verschillende partijen hebben op het voorstel van de Europese Commissie gereageerd. In deze paragraaf richten we ons op de EDPS en de Art. 29 Working Party.

Voordelen meldplicht
De Art. 29 Working Party en de EDPS staan achter de introductie van een meldplicht. Afgaande op ervaringen in de Verenigde Staten, is de EDPS van mening dat een meldplicht positieve effecten heeft op de bescherming van persoonsgegevens en privacy. Een meldplicht:

- bevordert de 'accountability' van de organisaties voor de gegevens die zijn verloren of gecompromitteerd;
- is een factor die organisaties die persoonsgegevens beheren motiveert om te investeren in veiligheidsmaatregelen;
- draagt bij aan het uitvoeren van betrouwbare statistische analyses om te bepalen wat de meest effectieve veiligheidsmaatregelen zijn;
- maakt burgers bewust van de risico's van gegevensverlies en helpt hen om deze risico's te beperken.

[1] Deze definitie is afkomstig uit het Framework Directive 2002/21/EC, de basis voor het Europese wetsbestel voor elektronische communicatiediensten. De termen *electronic communications network* en *public communications network* zijn gedefinieerd in Artikelen 2 a en d van Framework Directive 2002/21/EC

Maar…

Hoewel de EDPS en de werkgroep duidelijk voordelen zien van een meldplicht, vinden zij dat een aantal aspecten door de Commissie onvoldoende aan de orde zijn gesteld.

Vergroting reikwijdte

De EDPS en de werkgroep pleiten voor een vergroting van de reikwijdte van de meldplicht. De plicht zou moeten gelden voor alle diensten van de informatie-maatschappij, zodat de meldplicht ook van toepassing wordt op bijvoorbeeld online banken, online bedrijven en online aanbieders van gezondheidsdiensten als verzekeraars (zie box 'Wat zijn diensten van de informatiemaatschappij?').[1] Volgens de EDPS lopen gebruikers van netwerk-websites als Facebook en Hyves juist het meeste risico.

Onduidelijkheid privaat-publiek

De EDPS en de werkgroep wijzen daarnaast op de onduidelijkheid die bestaat over de betekenis van de gebruikte begrippen *public communications network* en *electronic communications services*[2]. Internet services zijn steeds vaker een mix van openbare en private elementen. Daarom is het vaak niet helder op welke organisaties de richtlijn van toepassing is. Bovendien is de definitie niet van toepassing op de niet-openbare netwerken en databases met persoonsgegevens die overheidsorganisaties beheren.

Bijvoorbeeld, is het verschaffen van internettoegang aan 30.000 studenten door een universiteit een openbaar of privaat netwerk?

De werkgroep roept de Commissie daarom op om duidelijkheid te verschaffen over deze begrippen. De EDPS vindt dat ook semi-openbare netwerken onder de richtlijn moeten vallen, bijvoorbeeld universiteiten en hotels die klanten een internetverbinding aanbieden[3].

All persons concerned

De Art. 29 Working Party voegt hieraan toe dat instanties niet alleen *subscribers* op de hoogte zouden moeten stellen, maar *all persons concerned*[4]. Hierdoor zouden ook ex-abonnees moeten worden gewaarschuwd. Daarnaast zou de nationale toezichthouder in sommige gevallen burgers moeten waarschuwen.

[1] Opinie WP 150, p. 2 en 3.
[2] De termen *electronic communications network* en *public communications network* zijn gedefinieerd in Artikelen 2 a en d van Framework Directive 2002/21/EC.
[3] Advies EDPS, p.6.
[4] Opinie WP 150, p. 3.

Wat zijn diensten van de informatiemaatschappij?

Artikel 3:15d lid 3 BW: *Elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn.*

Ofwel, alle activiteiten met een economisch karakter die online worden verricht. Het begrip 'economisch karakter' wordt ruim opgevat. De dienst moet 'gewoonlijk' tegen vergoeding worden verricht, wat niet uitsluit dat die gratis kan zijn voor de gebruiker en gefinancierd wordt door reclame of sponsoring.

Voorbeelden:

- e-commerce sites (Wehkamp.nl, Bol.com)
- internetbankieren
- gratis diensten (on-linedagbladen, forums, Facebook, Hyves, MySpace)
- online ontspanning (YouTube, online games, virtuele museumbezoeken)
- technische diensten die als tussenpersoon optreden (het verschaffen van toegang tot een communicatienetwerk, web hosting, elektronisch berichtenverkeer)
- certificeringsdiensten (elektronische archivering, aangetekende verzending, tijdsregistratie en handtekening)
- online zorgproviders
- telefoonboeken en zoekmachines (Google)

Bronnen: www.ejure.nl, Internet Observatory[1], Europees Parlement[2]

13.4 Voorstel Europees Parlement (September 2008)

Op 24 september 2008 stemde het Europees Parlement over de voorgestelde meldplicht. Het voorstel van het Europees Parlement gaat verder dan dat van de Commissie.

Grotere reikwijdte

Het voorstel van het Parlement vertoont duidelijk parallellen met de reacties van EDPS en de Art. 29 Working Party op de volgende punten:

- vergrootte reikwijdte:
  a) *alle* diensten van de informatiemaatschappij
  b) voor zowel openbare als private netwerken
- veiligheidsinbreuk melden aan *alle* betrokken personen, niet alleen abonnees

[1] Internet Observatory: Démoulin, M., Hervé, J., Bespreking van de wetten betreffende diensten van de informatiemaatschappij (CRID, 2003) Website: http://www.internet-observatory.be/internet_observatory/pdf/legislation/cmt/law_be_2003-03-11_cmt_nl.pdf

[2] Website Europees Parlement, Artikel: Telecoms: better services for consumers and a safer internet (24 september 2008) Website: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20080924+ITEMS+DOC+XML+V0//EN&language=EN#sdocta13

Introductie 'drietrapsraket' en bijzonder risico

Nieuw aan het voorstel van het Europees Parlement is de introductie van een 'drietrapsraket', waarin de procedure voor melding wordt gevat, en bijzonder risico. Het Europees Parlement werkt hierbij de grotere rol van de nationale toezichthouders verder uit. De voorgestelde procedure ziet er als volgt uit:

Stap 1. Alle veiligheidsinbreuken melden aan de nationale toezichthouder
Stap 2: in geval van *imminent and direct danger* melding aan de betrokkenen.
Stap 3. Hiernaast worden organisaties verplicht jaarlijks aan de betrokken burgers te rapporteren over alle inbreuken, genomen maatregelen en aanbevelingen voor burgers.

Hieronder wordt elke stap nader toegelicht.

Stap 1

De eerste stap van de drietrapsraket is het melden van *alle* veiligheidsinbreuken aan de nationale toezichthouder. De melding moet zo snel mogelijk geschieden.

Stap 2

Als dit volgens de toezichthouder inderdaad het geval is, moet de provider de veiligheidsinbreuk alsnog aan alle betrokken personen melden. Wanneer een provider na een veiligheidsinbreuk *zelf* constateert dat er sprake is van *imminent and direct danger* voor de gebruiker, moet hij dit, naast melding aan de nationale toezichthouder, direct zo snel mogelijk aan de betrokken personen melden.

Stap 3

Als derde trap van de procedure stelt het Europees Parlement voor dat providers jaarlijks alle veiligheidsinbreuken in een verslag rapporteren aan de gebruikers (3). Het verslag moet de maatregelen omvatten die de provider nam om de inbreuk aan te pakken alsook aanbevelingen voor de getroffen gebruikers over hoe hun data te beschermen. Dit verslag moet transparantie bieden over hoe providers met veiligheidsinbreuken omgaan.

Introductie bijzonder risico: compromis

De introductie van melding op basis van *imminent and direct danger* is het resultaat van een compromis tussen de conservatieven en socialisten in het Europees Parlement, blijkt uit interviews. Socialisten stelden voor om veiligheidsinbreuken te melden aan zowel de nationale toezichthouder als de betrokken personen. Conservatieve partijen waren van mening dat het niet nodig is om burgers van *alle* inbreuken op de hoogte stellen. Het compromis houdt in dat betrokken personen alleen worden ingelicht wanneer er sprake is van bijzonder risico. Hoe bijzonder risico gedefinieerd wordt, is echter nog niet duidelijk.

Alle veiligheidsinbreuken?

Het is op dit moment niet duidelijk of de Europese Commissie onder de grondslag melding van 'alle veiligheidsinbreuken' net als het Parlement *alle* inbreuken bedoelt. Volgens een respondent heeft de EC de grondslag van melding juist helder afgebakend, zodat niet alle inbreuken hoeven te worden gemeld.

Geen minimum aantal gedupeerden
Het voorstel van het Europees Parlement bevat geen minimum aantal gedupeerden als basis voor melding. Uit interviews blijkt dat het EP meer waarde hecht aan de soort gegevens die gevaar lopen dan het aantal gedupeerden. Ook kunnen door een minimum aantal vast te stellen kleinere bedrijven worden uitgesloten van de plicht een veiligheidsinbreuk te melden.

Geen boete
Het voorstel van de Commissie bevat geen boete als sanctie voor bedrijven die zich niet aan de meldplicht houden. Ook het EP heeft geen boetebevoegdheid opgenomen. Ten eerste is het EP niet bevoegd om strafmaatregelen te implementeren. Uit de interviews komt echter ook de motivatie naar voren dat het EP bedrijven niet de kans wil geven om de meldplicht 'af te kopen'.

13.5 Aangepast voorstel Europese Commissie en besluit Europese Telecomraad (November 2008)

Op 6 november 2008 bracht de Europese Commissie een aangepast voorstel voor een meldplicht uit; op 27 november 2008 kwam de Europese Telecomraad om het telecompakket te accorderen. De *Europese Commissie* en de *Raad* stellen voor dat dienstaanbieders in alle gevallen *zelf* bepalen of een veiligheidsinbreuk aan de betrokkenen moet worden gemeld: de toezichthouder krijgt in de voorstellen van de EC en de Raad deze bevoegdheid niet. Daarnaast willen zowel de EC als de Raad de reikwijdte van de meldplicht beperkt houden en deze niet verder laten gaan dan de organisaties die nu vallen onder de Europese telecomwetgeving (ISP's en telecombedrijven).

Het is mogelijk dat het Europees Parlement het telecompakket nog amendeert en de meldplicht wil verbreden tot alle diensten van de informatiemaatschappij. Daarnaast is het op dit moment niet duidelijk of de Europese Commissie onder de grondslag melding van 'alle veiligheidsinbreuken' net als het Parlement *alle* inbreuken bedoelt. Volgens een respondent heeft de EC de grondslag van melding juist helder afgebakend, zodat niet alle inbreuken hoeven te worden gemeld.

In februari 2009 neemt de Raad een volgende, formele beslissing. In maart stemmen de relevante commissies van het EP over de meldplicht. Uiterlijk eind april 2009 zal het EP plenair stemmen over het dan voorliggende voorstel.

14 Duitsland

Wat	Voorstel voor meldplicht tegelijk ingevoerd met vrijwillige audits in herziene privacy wetgeving (Bundesdatenschutzgesetz, BDSG)
Ingangsdatum	December 2008; indien wetsvoorstel niet aangenomen, uitstel van 1 of 2 jaar door verkiezingen
Wet	Audits en keurmerk: Ontwerp herziene BDSG, Versie 22 oktober 2008, Artikel 2, §1 en §8 Meldplicht: Idem, Artikel 1, §44a, Artikel 2, §19
Doel	Bevorderen aandacht van bedrijven en burgers voor bescherming persoonsgegevens
Voor welke organisaties	federale overheden; overheden van de Länder; private data controllers
Welke gegevens	bijzondere persoonsgegevens
Grondslag melding	melding wanneer gegevens onrechtmatig zijn verspreid of op onrechtmatige wijze bekend zijn geworden bij derden en er mogelijk sprake is van ernstige schade voor betrokken burgers
Aan wie melden	In ieder geval aan verantwoordelijke toezichthouder en betrokkenen
Handhaving	Verantwoordelijke data beschermingsautoriteit; boete bij niet-melding
Bijzonderheden	Een aantal elementen van de meldplicht zijn nog onderwerp van discussie. Als het wetsvoorstel in de huidige vorm in december 2008 wordt aangenomen, loopt Duitsland wat betreft de implementatie en scope van de meldplicht voor op de Europese Unie.

14.1 Aanleiding

De discussie over de introductie van een meldplicht in Duitsland is aangewakkerd door een reeks veiligheidsinbreuken en schandalen in 2008. Daarvoor was er al wel enige discussie over het invoeren van een meldplicht.
Deze discussie was geïnitieerd door de Duits toezichthouders, die van mening waren dat Duitsland dezelfde soort wetgeving moest implementeren als de Verenigde Staten.
Ook de herziening van de telecomwetgeving op Europees niveau heeft invloed gehad.

Het belangrijkste incident was een schandaal bij T-Mobile (Deutsche Telekom) waar uit een interne inspectie bleek dat een werknemer in 2006 17 miljoen gegevens had gekopieerd en doorverkocht. De geheime telefoonnummers van VIP's en politici maakten deel uit van deze gegevens. T-Mobile was op de hoogte van dit incident, maar heeft het nooit gemeld aan de betrokkenen.

14.2 Discussie

De dataschandalen hebben de discussie over de reikwijdte van een meldplicht verbreed: moet een meldplicht niet van toepassing zijn op alle bedrijven in plaats van alleen de telecomsector? De bancaire sector staat aarzelend tegenover een meldplicht met zo'n brede scope: de financiële crisis heeft het vertrouwen van consumenten al ernstig geschaad. Banken vrezen dat als zij veiligheidsinbreuken openbaar moeten maken het vertrouwen nog

verder afneemt. Een ander bezwaar dat niet alleen van de bancaire sector komt, is de administratieve last. Maar volgens respondenten wordt aan dit laatste tegenargument na de dataschandalen nog weinig waarde gehecht.

In Duitsland lijkt de invoering van een meldplicht verder brede steun te hebben, mede door recente dataschandalen. De discussie richt zich op de inhoud als kwesties wie de ernst van de veiligheidsinbreuk bepaalt en of alle betrokkenen moeten worden geïnformeerd of alleen een toezichthouder. Een belangrijke vraag is hoe de meldplicht moet worden gehandhaafd.

14.3 Inhoud audits en meldplicht

Duitsland kent nog geen meldplicht (*Informationspflicht)*. Een ontwerp meldplicht is recentelijk geïntroduceerd bij de herziening van de federale privacy wetgeving, de Bundesdatenschutzgesetz (BDSG).

Achtergrond federale Bundesdatenschutzgesetz
De federale BDSG functioneert naast de afzonderlijke databeschermingswetten van de 16 Länder. De BDSG, die inging in 2001, is het resultaat van de aanpassing van de bestaande, Duitse data beschermingswetgeving naar aanleiding van de implementatie van EU Directive 95/46/EC. De wet regelt het gebruik en de verwerking van data door bedrijven en definieert de rechten van individuen wat betreft bijvoorbeeld inzage van data. Daarnaast voorziet de BDSG in zelfregulering door bedrijven door het aanstellen van interne *privacy information officers* en door externe monitoring door de data autoriteiten. De aanleiding voor de meest recente herziening van de BDSG is om problemen op te lossen met onnodig gebruik van persoonsgegevens voor commerciële doeleinden door bedrijven.

Doelgroep
De voorgestelde meldplicht zou gelden voor de federale overheid, de overheden van de Länder (voor zover deze niet zelf wetgeving voor data bescherming hebben geïmplementeerd) en private data controllers, ofwel alle ondernemingen die persoonsgegevens verzamelen, beheren of verwerken. Daarmee is de scope van de audits en de meldplicht breder dan op Europees niveau, waar de voorgestelde meldplicht wordt beperkt tot de telecomsector (zie case study Europese Unie).

Soort gegevens
Uit interviews en de ontwerp-artikelen komt naar voren dat de voorgestelde meldplicht zou worden beperkt tot ‘bijzondere’ persoonsgegevens. Hieronder zouden kunnen vallen gegevens waar bijvoorbeeld een ambtsgeheim voor geldt, zoals medische en criminele dossiers, en creditcard- en bankgegevens[1].

Grondslag voor melding
Federale overheden, de overheden van de Länder en private data controllers zouden melding moeten maken aan de toezichthouder van ‘ernstige veiligheidsinbreuken’, komt uit interviews naar voren. Dit houdt in dat ’besondere’ persoonsgegevens onrechtmatig zijn ver-

[1] Ontwerp herziene BDSG, Versie 22 oktober 2008, Artikel 1, §44a

spreid of op onrechtmatige wijze bekend zijn geworden bij derden en er mogelijk sprake is van ernstige schade voor betrokken burgers.

Aan wie melden en hoe?
Het is op dit moment nog niet helder aan wie ondernemingen een inbreuk moeten melden en in welke vorm dat dient te geschieden. De betreffende ontwerpartikelen in de BDSG stellen dat organisaties de betrokken burgers en de verantwoordelijke data autoriteit op de hoogte moeten stellen[1]. Op federaal niveau is dit de *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit* (BfDI); op het niveau van bijvoorbeeld de deelstaat Beieren is dit de *Bayerische Landesbeauftragte für den Datenschutz*. De melding aan betrokken burgers moet volgens het betreffende ontwerp-artikel een toelichting bevatten over de aard van het gegevensverlies en aanbevelingen om schade te beperken[2].

Vrijwillige audits
De meldplicht wordt mogelijk tegelijk ingevoerd met vrijwillige data beveiligingsaudits (*Datenschutzaudits*) voor ondernemingen. Ondernemingen kunnen de daarvoor verantwoordelijke autoriteit (*Kontrollstelle)* verzoeken om een audit uit te voeren van hun beveiligingsprotocollen en –systemen[3]. Indien de beveiliging aan de voorgeschreven eisen voldoet, krijgt de onderneming een keurmerk, het *Datenschutzauditsiegel.* Omdat de audits niet verplicht worden, is de verwachting dat ondernemingen met elkaar gaan concurreren op het gebied van zorgvuldige omgang met persoonsgegevens[4]. De vrijwillige audits bouwen verder op de hoge mate van zelfregulering door het bedrijfsleven bij privacy en gegevensbescherming.

14.4 Handhaving

Een meldplicht zonder sancties is weinig effectief, is de heersende opinie. Maar het is momenteel nog de vraag hoe sancties moet worden vormgegeven: middels boetes en/of publicatie van veiligheidsinbreuken? In de ontwerp BDSG staat dat wanneer degene die een veiligheidsinbreuk ‘nicht, nicht richtig, nicht vollstandig oder nicht rechtzeitig’ meldt aan de data autoriteit een boete krijgt. De boete bedraagt maximaal € 300.000[5]. Omdat de manier van sanctioneren op dit moment nog onderwerp van discussie is, is het mogelijk dat dit nog verandert.

14.5 Wat volgt?

Het Parlement stemt naar verwachting in december 2008 over de herziene wet. Het is niet zeker dat de hierboven beschreven inhoud in deze vorm wordt aangenomen. Als het pakket niet wordt aangenomen, kan aanname van de herziene BDSG en daarmee de audits en de meldplicht waarschijnlijk nog één of twee jaar duren. Volgend jaar vinden namelijk eerst verkiezingen plaats in Duitsland.

[1] Idem
[2] Idem
[3] Ontwerp herziene BDSG, Versie 22 oktober 2008, Artikel 2, §1 en §8.
[4] Entwurf BDSG (Stand 22 oktober 2008), Begrundung, A. Allgemeiner Teil, I Ziel und Einhalt des Entwurfs
[5] Idem, Artikel 2, § 17.

15 Verenigd Koninkrijk

Wat	Boetebevoegdheid ICO in geval van schending privacy wetgeving
Ingangsdatum	Mei 2008
Wet	Criminal Justice and Immigration Act, Art. 144 Data Protection Act, Art. 55A t/m E
Doel	Afschrikmiddel voor data controllers om DPA te schenden
Voor welke organisaties	data controllers
Welke gegevens	Persoonsgegevens
Grondslag voor boete	In geval van schending van sectie 4(4) van de Data Protection Act door data controller[1]
Aan wie melden	Nvt: in de UK zijn data controllers volgens de Data Protection Act niet verplicht om gegevensverlies te melden.
Handhaving	De nationale toezichthouder, Information Commissioner's Office (ICO)
Bijzonderheden	In de financiële sector heeft de Financial Services Authority (FSA) al sinds 2000 een boetebevoegdheid.

15.1 Discussie

Op dit moment kent het Verenigd Koninkrijk geen meldplicht, alleen een boetebevoegdheid in geval van schending van de Data Protection Act. De discussie over de invoering van een meldplicht in het Verenigd Koninkrijk vindt plaats op twee niveaus:

- brede, maatschappelijke discussie over de noodzaak van de invoering van een meldplicht die geldt voor zowel overheden als het bedrijfsleven naar aanleiding van een reeks grootschalige veiligheidsinbreuken in de UK;
- discussie op overheidsniveau op basis van het voorstel van de Europese Commissie om een meldplicht op Europees niveau in te voeren (zie casestudy Europese Unie).

De discussie over de noodzaak en de inhoud van een meldplicht is nog niet uitgekristalliseerd in het Verenigd Koninkrijk. Als gevolg van het grote aantal veiligheidsinbreuken, wordt de invoering van een meldplicht breed gedragen door de nationale consumentenorganisatie (NCC). De Information Commissioner's Office (ICO) is voorzichtig over het invoeren van een meldplicht.
Argumenten voor een meldplicht zijn:

- consumenten hebben het recht te weten dat hun persoonsgegevens gevaarlopen;
- verlagen van het risico voor consumenten door hen voor te lichten over preventieve maatregelen;

De Britse nationale consumentenorganisatie NCC heeft er (samen met andere consumentenorganisaties in Europa) bij de Europese Commissie op aangedrongen een meldplicht te implementeren.

[1] Sectie 4(4) uit de DPA stelt data controllers zich aan deze wet moeten houden: *Subject to section 27(1), it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.*

- melding aan de autoriteiten verbetert regulering en doet kennis over veiligheidsinbreuken toenemen; ook stelt het de toezichthouder in staat bedrijven te begeleiden in geval van een veiligheidsinbreuk en om hen te helpen dit in de toekomst te voorkomen;
- waarschuwing voor bedrijven om meer aandacht aan de beveiliging van hun netwerk te schenken.

Geluiden tegen de meldplicht komen onder andere uit de ICT-sector. Partijen in de ICT zien onder andere aansprakelijkheid als probleem. Een ander tegengeluid uit de ICT-sector is de voorkeur voor de nadruk op preventie en de verbetering van veiligheidsmaatregelen[1].

De ICO pleit voor heldere criteria over hoe, in welke gevallen en wat te melden. Het huidige EU-voorstel voor een meldplicht vindt de ICO echter 'too prescriptive and too burdensome'[2]. De ICO ziet de grote hoeveelheid bureaucratie voor bedrijven als nadelig gevolg. Dit zonder enig bewijs dat een meldplicht veiligheidsinbreuken vermindert of voorkomt. Ook is de ICO bezorgd dat consumenten een overdaad aan meldingen ontvangen. Om deze redenen is ICO er niet voor meldplichten uit de Verenigde Staten klakkeloos over te nemen in Europa.

15.2 Inhoud boetebevoegdheid

Het Verenigd Koninkrijk kent dus (nog) geen meldplicht, maar wel een boetebevoegdheid onder de Data Protection Act (DPA). Deze wet uit 1998 reguleert de bescherming van persoonsgegevens en privacy van consumenten. De DPA vereist onder andere dat persoonsgegevens veilig moeten zijn bij de data controller. Sinds mei 2008 is de Information Commissioner bevoegd om bedrijven en organisaties een boete op te leggen indien zij de DPA schenden[3]. Ook een veiligheidsinbreuk of gegevensverlies kunnen zo leiden tot een boete.

De Financial Services Authority (FSA) is sinds 2000 bevoegd om financiële instanties te beboeten indien zij gegevens van consumenten onvoldoende beveiligen.

In deze paragraaf gaan we nader in op deze wet en de daaruit voortvloeiende bevoegdheden van de ICO.

Doelgroep

De DPA geldt voor alle *data controllers,* ofwel alle personen en organisaties die persoonsgegevens voor een bepaald doel be- of verwerken[4]. Data controllers zijn onder de DPA verplicht zich aan te melden bij de Privacy Commissioner. Elke aanmelding wordt geregistreerd in een openbaar register, zodat burgers kunnen nagaan welke organisaties hun persoonsgegevens verwerken en op welke manier zij dat doen[5]. Registratie kost £ 35 per jaar[6].

[1] Story URL: http://news.zdnet.co.uk/security/0,1000000189,39291944,00.htm (20 november 2008)
[2] Information Commissioner turns up the heat on data breach culprits (30 oktober 2008).
[3] De boetebevoegdheid in de DPA werd geïntroduceerd middels de herziening van de Criminal Justice and Immigration Act in 2008.
[4] Hier vallen niet de Crown Estate Commissioners onder of het Koninklijk Huis.
[5] Register ICO: http://www.ico.gov.uk/tools_and_resources/register_of_data_controllers.aspx (20 november 2008)
[6] Website ICO en: Information Commissioner turns up the heat on data breach culprits (30 oktober 2008).

Een eventuele meldplicht zou volgens de ICO ook moeten gelden voor alle data controllers en niet alleen voor een bepaalde sector, zoals nu in Europa wordt voorgesteld.

Soort gegevens
De DPA is van toepassing op persoonsgegevens[1]. Een meldplicht zou ook van toepassing moeten zijn op persoonsgegevens.

Grondslag voor boete
De grondslag voor de boete is momenteel breed gedefinieerd in de Criminal Justice and Immigration Act. Deze wet stelt dat de Privacy Commissioner een boete kan opleggen in geval van opzettelijke schending van sectie 4(4) van de DPA, ofwel wanneer een organisatie zich niet aan de privacy wetgeving houdt. De boete wordt opgelegd wanneer de data controller wist dat de schending van de wet redelijkerwijs wezenlijke schade tot gevolg kon hebben voor betrokkenen, maar geen maatregelen heeft genomen om de schending te voorkomen. De Privacy Commissioner stelt zelf een richtlijn op hoe hij deze grondslag interpreteert.

> Sectie 4(4) stelt dat: 'it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller'.

Terwijl in de media is bericht over een boetebevoegdheid in geval van een veiligheidsinbreuk of gegevensverlies, staat dit zo niet letterlijk in de wet[2]. Omdat de DPA van data controllers onder andere verlangt dat de door hem beheerde persoonsgegevens *secure* zijn, is het wel mogelijk dat een veiligheidsinbreuk leidt tot een boete.

15.3 Procedure

Als de Privacy Commissioner het nodig vindt een boete op te leggen, verplicht de wet hem om de data controller eerst een *notice of intent* te sturen. De data controller kan gedurende een zekere periode bij het *Information Tribunal* in beroep gaan tegen de boete zelf en tegen de hoogte van het bedrag.

15.4 Handhaving

Als een data controller weigert te betalen, kan de boete worden afgedwongen door de rechter. De hoogte van de boete is momenteel relatief laag; het gaat volgens respondenten vooral de imagoschade als gevolg van een boete. De maatregelen die de ICO tegen data controllers neemt, worden op de ICO website gepubliceerd.

[1] Persoonsgegevens zijn in de DPA als volgt gedefinieerd: ' (…) data which relate to a living individual who can be identified - (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.

[2] Bijvoorbeeld artikel in ComputerWeekly.com: ICO given new powers to fine organizations for data losses (May 2008)

Naming & shaming

Op de website van de Privacy Commissioner is te lezen welke stappen de ICO onder andere tegen de politie, overheidsdepartementen, telecom- en thuiswinkelbedrijven heeft genomen na schending van de privacy wetgeving. Ook de uitkomst van deze stappen wordt gepubliceerd. Op 25 januari bevond de ICO bijvoorbeeld Marks & Spencer schuldig aan het schenden van de DPA, omdat een laptop van deze winkelketen was gestolen met daarop gegevens van 26.000 werknemers. De laptop was niet beveiligd. Een half jaar later, valt te lezen op de website, is de *enforcement notice* weer ingetrokken: Marks & Spencer heeft gevolg gegeven aan de eis van de ICO om laptops te beveiligen (*laptop encryption)* [1].

Voordat de boetebevoegdheid werd geïntroduceerd in mei 2008, had de ICO naast publicatie van maatregelen al een aantal bevoegdheden om de DPA te handhaven:

- uitvoeren van audits en controles om te zien of een data controller zich aan de DPA houdt en persoonsgegevens goed verwerkt;
- *information notices* waarin de ICO informatie van een organisatie eist binnen een bepaalde periode;
- *enforcement notices* en *stop now* orders waarin de ICO een data controller verplicht zich aan de DPA te houden en daartoe acties te ondernemen;
- rechtelijk vervolgen van degenen die een misdrijf plegen in het kader van de DPA;
- rapportage aan het Parlement over belangrijke privacy issues.

ICO vraagt om meer bevoegdheden om veiligheidsinbreuken bij organisaties te voorkomen, zoals de mogelijkheid om onaangekondigd binnen te vallen bij bedrijven wanneer er een vermoeden bestaat dat zij een overtreding begaan[2].

15.5 Evaluatie

Hoewel in het VK organisaties niet verplicht zijn om veiligheidsinbreuken aan de Privacy Commissioner te melden, gebeurt dit in de praktijk wel. Binnen een jaar ontving de ICO 277 meldingen[3]. In de praktijk zijn er door de ICO echter nog nauwelijks boetes opgelegd voor veiligheidsinbreuken of gegevensverlies. De hoogte van de boete is namelijk nog niet vastgesteld door het Britse Departement van Binnenlandse Zaken. ICO verwacht dat de hoogte hetzelfde zal worden als voor de FSA, welke boetes kan opleggen van maximaal 10 procent van de omzet en dit ook doet. Een belangrijk voorbeeld van een boete die de FSA heeft opgelegd is de boete van bijna £ 1 miljoen voor *Nationwide Building Society* vorig jaar. Nationwide had onvoldoende veiligheidsmaatregelen genomen, bleek uit een controle.

[1] Website ICO, pagina *Enforcement:* http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx (20 november 2008)
[2] Information Commissioner turns up the heat on data breach culprits (30 oktober 2008).
[3] Information Commissioner turns up the heat on data breach culprits (30 oktober 2008). 28 inbreuken vonden plaats bij de centrale overheid; 75 bij de NHS en andere gezondheidsorganisaties en 80 bij het bedrijfsleven.

Bijlage 1 Overzicht respondenten

De contactpersonen van de geselecteerde landen en staten zijn meerdere malen via e-mail en telefonisch benaderd met het verzoek om deel te nemen aan het onderzoek. Uiteindelijk hebben wij in totaal 18 interviews gehouden. Hiervan zijn binnen de Europese Unie twee interviews gehouden; in Nederland is gesproken met 7 experts.

Buitenland:

Alexander Alvaro
MEP Duitsland, rapporteur Committee on civil liberties justice and home affairs
Europees Parlement, Brussel

Atle Årnes
Senior adviseur
Datatilsynet, Noorwegen

Laurent Beslay
Wetenschappelijk adviseur, vertegenwoordiger EDPS in technologie werkgroep EU
European Data Protection Supervisor (EDPS), Brussel

Karen Curtis
Privacy Commissioner
Office of the Privacy Commissioner (OPC), Australië

Elizabeth Denham
Assistant Privacy Commissioner
Office of the Privacy Commissioner, Canada

Alexander Dix
Regeringscommissaris Datenschutz und Informationsfreiheit in Berlijn
Berliner Beauftragter für Datenschutz und Informationsfreiheit, Berlijn, Duitsland

James Earl
Executive Director
Nevada's Technological Crime Advisory Board, Nevada, Verenigde Staten

David Evans
Senior data protection practice manager
Information Commissioner's Office (ICO/GSI), Verenigd Koninkrijk

Pam Greenberg
Attorney
National Conference of State Legislatures (NCSL), Denver Office, Verenigde Staten

Joanne McNabb
Chief Californië Office of Privacy Protection
Californië, Verenigde Staten

Gina Marie Stevens
Legislative Attorney
Congressional Research Service (CRS), Washington DC, Verenigde Staten

Nederland:

Geo Aldershof
Secretaris Criminaliteitsbeheersing en Veiligheid
VNO/NCW

Ronald van den Broek
Juridisch adviseur internetveiligheid
OPTA

Jan Grijpink
Raadadviseur informatiestrategie, Dir. Algemene Justitiële Strategie, Ministerie van Justitie;
Bijzonder hoogleraar Informatiekunde, Faculteit Bètawetenschappen, Universiteit Utrecht;
Adviseur Het Expertise Centrum (HEC).

Nico van Eijk
Bijzonder hoogleraar Media- en Telecommunicatierecht
Instituut voor Informatierecht (IVIR), Universiteit van Amsterdam

Bert-Jaap Koops
Hoogleraar regulering van technologie
Centrum voor Recht, Technologie en Samenleving (TILT), Universiteit van Tilburg

Ronald Leenes
Universitair hoofddocent recht en regulering van technologie
Centrum voor Recht, Technologie en Samenleving (TILT), Universiteit van Tilburg

Sjoera Nas
Internet- en telecomexpert
College Bescherming Persoonsgegevens (CBP)

Bijlage 2 Checklist interviews buitenland

Deze bijlage bevat de Engelstalige vragenlijst voor respondenten in landen met een meldplicht. De vragenlijst is steeds toegesneden op respondenten met specifieke kennis en respondenten afkomstig uit een land met discussie over invoering van een meldplicht.

A. Background breach law

1. Could you please describe the reasons for adopting legislation that obliges organizations to notify in case of data loss?
2. We assume that the notification, before its adoption, has been under discussion.
   - What arguments were brought forward *favoring* notification?
   - What arguments were brought forward *opposing* notification?
3. Have alternatives to a notification been considered? If so, which alternatives? What have been the reasons to opt for a notification instead of the alternative(s) mentioned?
4. To what extent was information available about the number of data security breaches in the period *prior to* the law?

B. Contents of the breach law

5. What organizations are subjected to the law? Why these organizations (and not others)?
6. What type of data are covered by the notification law? Why these data?
7. Does the notification law only concern unsecured data, or also encrypted data?
8. Which law covers the notification?
9. When (under what circumstances) does an organization have to notify dataloss? In case of (more than one answer possible):
   - any data security breach
   - a minimum number of lost data or of victims (citizens or clients)
   - the seriousness of the system breach
   - acute risk for citizens or clients
   - the type of data that are lost
   - other, namely …….
10. What were the considerations which have led to selecting these criteria?
11. In what way(s) has/have the criteria mentioned been put into operation? For example, how is an 'acute risk' of the security breach determined?

C. Procedures for notifying a data security breach

12. What steps does a business or organization under the law have to take in case of data loss?
    a) Where (at which authority) does an organization have to notify data loss?
    b) What were the reasons for selecting this authority?
    c) In what way does data loss have to be notified (written notice, electronic notice)?
    d) What is the deadline for notification after dataloss has taken place?
    e) In what way(s) are customers being informed about data loss?

13. What happens after a security breach has been notified?
14. Is there any central, independent office for citizens to report a data loss or to seek further information? Why/why not?

D. Enforcement / observance

15. In what way(s) is the law being enforced? (more than one answer possible):
    a) Fine in case of not notifying
    b) Fine in case an organization under the law fails to notify data loss within a certain term.
    c) Obligatory improvement of security systems for organizations under the law.
    d) Obligatory audits of security systems for organizations under the law.
    e) Fine in case of unsatisfactory safeguards.
    f) Obligation for organizations under the law to periodically report on data loss to responsible agencies or to clients.
    g) Other: …….
16. What were the reasons for opting for these forms of enforcement?
17. What authority is (or which authorities are) responsible for enforcing the law?
    - What are their position, status and powers?
    - What sanctions can they impose?
    - Have these sanctions actually been imposed? (If so, how often?)
18. Do you have any information on the extent to which the law is being observed by organizations under the law?

E. Evaluation

19. What objectives were formulated at the adoption of the legislation?
    - To what extent have these objectives been reached?
    - Has the law led to any other (unintended) results?
    - Did the law have any other (possibly unforeseen) consequences?
20. What are the advantages and the disadvantages of the law?
21. Has the law proven to be an effective means to prevent data security breaches?

Final questions

22. Do you know of any relevant literature or documents for us to read?

Bijlage 3 Checklist interviews Nederland

A. Achtergrond

1 Wat is volgens u de aanleiding van het voorstel voor een meldplicht in Nederland?
2 In welke mate zijn gegevens bekend over de omvang van veiligheidsinbreuken en gegevensverlies in Nederland?
3 Wat zijn volgens u argumenten voor en tegen een meldplicht in Nederland?
4 Zijn er volgens u alternatieven voor een meldplicht? Zo ja, welke? Wat is uw mening over *vrijwillige* meldplicht, zoals in Canada, Australië en Nieuw Zeeland bestaat?

B. Inhoud en vormgeving

Wat zou de **inhoud** van de meldplicht in Nederland moeten zijn, volgens u:

5 Voor welke organisaties zou de meldplicht gelden? Waarom deze organisaties?
6 Voor welke soort gegevens zou de meldplicht gelden, en waarom? Zou de meldplicht alleen voor onbeveiligde gegevens gelden of ook voor tot *encrypted* gegevens?
7 Onder welke wet zou de meldingsplicht worden ondergebracht? Waarom deze wet?
8 Wanneer zou een organisatie melding moeten maken van *data security breach* (meerdere antwoorden mogelijk)? In geval van of op basis van:
   a) iedere *data security breach*
   b) een minimum aantal verloren gegevens of gedupeerde burgers
   c) de ernst van de inbreuk in het systeem
   d) aantoonbaar risico voor de burger of klant
   e) de aard van de verloren gegevens
   f) Anders, namelijk:
9 Op grond van welke overwegingen heeft u een voorkeur voor de genoemde criteria?
10 Hoe zouden de genoemde criteria worden geoperationaliseerd? Ofwel, hoe kan bijvoorbeeld aantoonbaar risico of de ernst van de *security breach* worden vastgesteld en door wie?

C. Procedure

11 Wat moet een meldplichtig bedrijf doen wanneer deze melding moet maken van een *data security breach*? Welke stappen moet dit bedrijf nemen?
   a) Bij welke instantie(-s) zou een organisatie *data security breach* moeten melden? Waarom deze instantie(-s)?
   b) Welke vorm zou een melding hebben, en waarom deze vorm?
   c) Binnen welke termijn zou moeten worden gemeld?
   d) Hoe zouden klanten op de hoogte worden gesteld van een *data security breach*?

D. Handhaving / naleving

12 Hoe zou, volgens u, de meldplicht moeten worden gehandhaafd? (meerdere antwoorden mogelijk):
   a) Boete in geval van niet-melden
   b) Boete wanneer een meldplichtig bedrijf de *data security breach* niet binnen een bepaalde termijn bekend maakt
   c) Meldplichtige organisaties zijn verplicht de beveiliging van hun systemen aan te scherpen
   d) Audits van de beveiliging van systemen zijn verplicht voor meldplichtige organisaties
   e) Boete in geval van onvoldoende beveiliging
   f) Meldplichtige organisaties zijn verplicht periodiek te rapporteren over *data security data breaches* aan de verantwoordelijke instantie of de klant (voorstel Europees Parlement)
   g) Anders, namelijk…

13 Waarom is er een voorkeur voor de aangegeven vorm van handhaving?

14 Wie zou er volgens u aansprakelijk moeten zijn voor de kosten van een melding? Bijvoorbeeld, in geval van verlies van creditcardgegevens, moet de bank de kosten van vervanging van creditcards betalen of het bedrijf dat deze gegevens is kwijtgeraakt?

Tot slot

15 Kunt u ons relevante documentatie aanraden?

Research voor Beleid
Bredewater 26
Postbus 602
2700 MG Zoetermeer
tel: 079 322 22 22
fax: 079 322 22 12
e-mail: info@research.nl
www.research.nl