De meldplicht datalekken

De boete die een organisatie kan krijgen voor het niet op orde hebben van de beveiliging van persoonsgegevens kan per 1 januari 2016 oplopen tot € 820.000 en in uitzonderlijke situaties zelfs 10% van de netto-omzet. Voor het niet melden van een datalek is de maximale boete € 500.000 per overtreding. Daarnaast moeten de gedupeerden worden geadviseerd over de mogelijkheden tot beperking van de (eventuele) schade als gevolg van een datalek.

Herziene versie, 26 januari 2016 [v2.2] (definitief)

Realisatie: Aramis Jean Pierre, Gineke Kuipers en Ruud de Bruijn

Centrum voor Informatiebeveiliging en Privacybescherming, Domeingroep Privacy

Inhoudsopgave

Met het doel informatie-uitwisseling en kennisdeling te bevorderen, wil CIP onder andere 'good practices' ter beschikking stellen. Dit kunnen praktijkvoorbeelden zijn, handreikingen voor beleid, beschrijvingen van de stand van zaken in bepaalde ontwikkelingen, en dergelijke. De herkomst is van oorsprong een reflectie op een onderwerp door mensen in de CIP-kring, maar het kunnen ook notities zijn uit de praktijk van de CIP-organisaties die zonder verder commentaar worden gepubliceerd. De kern is dat de bijdragen altijd zijn gebaseerd op de expertise van de opstellers en deelnemende reviewers en/of het idee dat wat in één organisatie goed werkt, ook voor andere organisaties nuttig zou kunnen zijn. Soms is het resultaat dus de uitkomst van een groepsproces en in andere gevallen wordt iets 'as is' ter kennisneming of overname aangeboden. CIP heeft categorieën geformuleerd waarmee reikwijdte, intentie, status en/of draagvlak van CIP-publicaties wordt aangegeven. Deze publicatie valt in categorie 2: "becommentarieerde praktijk: een door meerdere professionals veralgemeniseerde praktijk als handreiking voor hergebruik binnen geïnteresseerde organisaties". Een nadere uitleg hiervan staat op www.cip-overheid.nl.

De CIP-documenten hebben geen ander doel dan kennisoverdracht en reflecteren niet noodzakelijk de opvattingen van alle contribuanten, CIP-deelnemers en/of alle CIP-partijen. Publicatie vindt plaats op zowel de openbare website www.cip-overheid.nl als de besloten community site https://cip.pleio.nl.

CIP-documenten kunnen van tijd tot tijd aanpassingen ondergaan of worden ingetrokken als gevolg van veranderde inzichten. De CIP-redactie streeft binnen haar mogelijkheden naar een zo actueel mogelijke status van de documenten. In de praktijk zal enige tijd verstrijken voordat wijzigingen kunnen zijn doorgevoerd. Suggesties voor aanpassingen kunnen ook door lezers worden aangedragen en worden altijd in behandeling genomen.

1. Inleiding

Sinds de inwerkingtreding van de meldplicht datalekken op 1 januari jl. zijn hierover al meerdere publicaties verschenen, vanuit verschillende perspectieven: algemeen informatief, gedetailleerd gericht op de afwikkeling van een datalek, of specifiek over de juridische en organisatiemaatregelen die nodig zijn om op eventuele schade als gevolg van datalekken te anticiperen. Dit document behandelt deze aspecten met de bedoeling organisaties bewust te maken van de wetgeving en haar mogelijke gevolgen. Op de geëigende plaatsen wordt voor verdieping verwezen naar toepasselijke publicaties van anderen. Wie zich er in verdiept komt erachter dat onder de nieuwe wetgeving veel meer incidenten een 'datalek' zijn dan de term zelf doet vermoeden, en dat hij er snel mee aan de slag zal moeten omdat er met name in de voorbereiding heel wat meer bij komt kijken dan op het eerste gezicht lijkt.

1.1 Wat komt aan de orde?

Dit document biedt een overzicht van de inhoud van de meldplicht datalekken en de belangrijkste implicaties voor organisaties. 'De meldplicht datalekken' heet voluit: *Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp)*. Wij houden het hier op 'de meldplicht' of 'de meldlicht datalekken'. Het Cbp heet inmiddels 'de Autoriteit Persoonsgegevens' (AP).

Er zijn twee andere ontwikkelingen die enige verwantschap hebben met deze meldplicht. Het betreft het wetsontwerp "Wet gegevensverwerking en meldplicht cybersecurity" en de Europese "Algemene Verordening Gegevensbescherming" (AVG). Beide worden in dit verband overigens summier besproken.
De meldplicht in het genoemde wetsontwerp is niet beperkt tot verwerkingen van persoonsgegevens en kent ook geen boetebepalingen. Het doel is schade als gevolg van 'cyberincidenten' (inbreuken in de IT) bij organisaties in de *vitale infrastructuur* te (helpen) repareren. Dit wetsontwerp kent een Europese verwant: de ontwerprichtlijn over netwerk- en informatiebeveiliging (NIB).

De AVG beoogt net als 'onze' meldplicht datalekken een betere en binnen de Europese Unie meer uniforme bescherming van de privacy van burgers. De Verordening bevat onder meer een vergelijkbare meld- en administratieplicht voor datalekken (personal data breaches), maar er zijn verschillen in definities, accenten en de hoogte van boetes. En: lidstaten kunnen of moeten toch nog op veel punten een eigen invulling geven.

1.2 Brondocumenten en interpretaties

Wij geven in deze publicatie de essentie van de meldplicht weer en wijzen op een aantal mogelijke consequenties. Wij benadrukken daarbij bepaalde aspecten en hebben een aantal accenten aangebracht. Maar de wettekst, de Memorie van toelichting, amendementen in het parlement en de aanwijzingen van de toezichthouder zijn de enige documenten die gelden voor de toepassing van de Meldplicht in de praktijk. Wat overigens niet wil zeggen dat zich daarbij geen interpretatievraagstukken zullen voordoen.

Op het internet zijn veel beschouwingen over de meldplichtproblematiek verschenen. Veel daarvan dateren echter van vóór het verschijnen van de AP-beleidsregels terzake. Omdat het niet zelden columns of artikelen zijn, zijn de teksten vaak niet aangepast aan de wijzigingen per 1 januari 2016. Het zijn niettemin vaak nog zeer bruikbare samenvattingen of bespiegelingen, maar probeer altijd wel de publicatiedatum te achterhalen en trek feitelijke informatie altijd na bij de AP.

Ons advies is om niet uitsluitend af te gaan (of uit te gaan) op (van) dit document en soortgelijke publicaties, maar zeer beslist ook de 'brondocumenten' te lezen en eventuele ontwikkelingen bij te houden, bijvoorbeeld in de rechtspraak of in Europees verband. In het Bronnenoverzicht hebben wij de verwijzingen naar de relevante documenten op een rijtje gezet.

1.3 Aantekeningen bij deze versie

Deze tweede versie is een herziening van het oorspronkelijke document nu de meldplicht op 1 januari 2016 in werking is getreden en de concept Richtsnoeren van het College Bescherming Persoonsgegevens definitief zijn gemaakt in de Beleidsregels van de Autoriteit Persoonsgegevens (AP). Ten opzichte van de eerder gepubliceerde (concept) Richtsnoeren bevatten de Beleidsregels significante wijzigingen.

De Wet gegevensverwerking en meldplicht cybersecurity moet nog definitief gemaakt worden. Het wetsvoorstel is naar de Raad van State gestuurd en onlangs ook naar de Tweede Kamer. De Raad heeft zich enigszins kritisch uitgelaten, onder ander door te stellen dat de wet overbodig zou zijn. Uit de eerste reacties vanuit het parlement valt nog niet veel op te maken.

De AVG is op 25 mei van dit jaar (2016) in werking getreden. Ook hier bleken op de valreep nog - soms verrassende - aanpassingen te zijn aangebracht in de uiteindelijke tekst van de Verordening. Uitgebreide behandeling is in dit bestek niet aan de orde, we beperken ons hoofdzakelijk tot opvallende kenmerken in relatie tot onze nationale meldplicht. Ook hier adviseren wij voorzichtig omgaan met internetbronnen: je komt nog veel beschouwingen tegen van (net) vóór de publicatie van de eindversie van de AVG. Deze teksten bevatten waardevolle informatie, maar let op de datum en ga altijd bij de AVG zelf te rade als je het precies en zeker moet weten.

Ten slotte een redactioneel-technische noot. De tekst van dit document bevat een aantal hyperlinks. Niet alle PDF-readers activeren echter de hyperlinks onder de tekst. Daarom geven wij de URL van een verwijzing ook nog voluit weer in het Bronnenoverzicht of in een voetnoot. Je moet de URL dan zelf in de adresbalk van een browser plakken.

2. Samenvatting

De *meldplicht datalekken* is op 1 januari 2016 van kracht geworden. Het doel van de meldplicht is het voorkomen van datalekken (ten gevolge van doorbreking van beveiligingsmaatregelen) en het beperken van de schade ervan voor betrokkenen[1]. Deze schade zou kunnen optreden als gevolg van een incident waarbij persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. De meldplicht is opgenomen in de Wet bescherming persoonsgegevens (Wbp) als een nieuw artikel 34a en geldt voor iedere verantwoordelijke voor de verwerking van persoonsgegevens, zowel in de private als publieke sector. De wet verplicht de verantwoordelijke tot het melden van een (ernstig) datalek aan de Autoriteit Persoonsgegevens (AP)[2] en in bepaalde gevallen ook aan de betrokkenen. Dit laatste is afhankelijk van de ernst van het datalek en de mogelijke gevolgen voor de betrokkenen. Voor financiële instellingen gelden andere, sectorspecifieke regels. Er zijn ook uitzonderingen op de meldplicht die te maken hebben met risicobeperkende maatregelen waardoor gelekte gegevens ontoegankelijk zijn gemaakt voor onbevoegden (bijvoorbeeld door volledige encryptie).

De meldplicht houdt in dat de verantwoordelijke voor de verwerking van persoonsgegevens de AP 'onverwijld' in kennis stelt van een datalek dat voldoet aan de volgende kenmerken:

- er is een inbreuk op de beveiliging als bedoeld in artikel 13 Wbp. Dit artikel stelt onder meer dat de verantwoordelijke verplicht is om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking; en
- de inbreuk leidt tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, dan wel tot een aanzienlijke kans daarop.

Hou rekening met het inrichten van een incidentenadministratie. Het is feitelijk nog onduidelijk welke incidenten moeten worden bijgehouden, maar de valkuil is dat je vooraf niet altijd weet of een incident onder de meldplicht valt of niet. Voorlopig lijkt hiervoor een bewaartermijn van minimaal 1 en in sommige gevallen minimaal 3 jaar te gelden.

De inbreuk kan in het verleden onopgemerkt hebben plaatsgevonden, maar uit de Beleidsregels van de AP[3] is op te maken dat onverwijld betekent "zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur *na de ontdekking*". Wordt die termijn niet gehaald dan moet de verantwoordelijke de vertraging kunnen motiveren.

Bij niet tijdige melding kan de AP:

- een (bindende) aanwijzing geven om alsnog te melden;
- een bestuurlijke (basis)boete opleggen tot maximaal €500.000 per overtreding.

De overtreding die hier wordt bedoeld is niet zozeer het datalek zelf, maar *het niet melden*[4]. Er zijn meer overtredingen die direct aan de meldplicht zijn gerelateerd en tot boetes kunnen leiden tussen de € 120.000 en € 500.000.
Een boete wordt in de regel niet opgelegd als niet éérst een bindende aanwijzing is gegeven. Maar in gevallen van opzet of ernstig verwijtbare nalatigheid kan de boete ook zonder meer direct worden uitgedeeld en zelfs hoger uitvallen (€ 820.000).

[1] Onder 'betrokkenen' verstaan we de personen van wie de gegevens zijn gelekt, d.w.z. de personen waarop de informatie betrekking heeft die in de betreffende gegevens is vervat; de betrokkene is niet de 'eigenaar' van de gegevens.
[2] De Autoriteit Persoonsgegevens is per 1-1-2016 de opvolger van het College Bescherming Persoonsgegevens (Cbp) en de toezichthouder voor de Meldplicht datalekken.
[3] Voluit: De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). Beleidsregels voor toepassing van artikel 34a van de Wbp. Autoriteit Persoonsgegevens, 8 dec 2015. Wij verwijzen ernaar met 'De Beleidsregels (van de AP)'.
[4] https://www.privacybarometer.nl/maatregel/41/Meldplicht_datalekken_en_uitbreiding_boetebevoegdheid.

De AP kan verzachtende dan wel verzwarende omstandigheden in aanmerking nemen en als gevolg daarvan afwijken van de standaardbedragen. Ook financiële omstandigheden kunnen van invloed zijn.
Over de lastig te doorgronden boeteclausule komen we nog te spreken in paragraaf 3.8.

Overigens is het doen van een melding niet per definitie voldoende voor vrijwaring van onderzoek en eventuele beboeting door de AP.

De meldplicht schrijft ook expliciet een zorgvuldige informatieverstrekking aan de betrokkenen voor. De verantwoordelijke moet de betrokkenen onverwijld in kennis stellen van de inbreuk als deze waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkenen.
De wet en de Memorie van Toelichting (MvT), en ook de Beleidsregels van de toezichthouder laten enige ruimte voor interpretatie, met name waar het de inschatting van risico of mogelijke schade voor betrokkenen betreft. Het is nog niet duidelijk hoe de toezichthouder hiermee omgaat. Het is ook mogelijk dat hierover jurisprudentie zal ontstaan.

Een datalek hoeft niet altijd een lek te zijn waarbij de vertrouwelijkheid wordt geschonden. Ook schending van de gegevens*integriteit* of *onbeschikbaarheid* van gegevens kan een datalek zijn in de zin van de wet. De centrale gedachte achter de meldplicht is immers bescherming van betrokkenen tegen schade die is gerelateerd aan verwerking van zijn persoonsgegevens.

Aan de inhoud van de melding wordt een aantal eisen gesteld. De Beleidsregels geven aan dat de kennisgeving aan de AP naast de feitelijke incidentmelding, de aard en de omvang ervan ook moet ingaan op onder meer:
- het wettelijk kader voor de melding (bijvoorbeeld Wbp, Telecomwet); contactgegevens, sector;
- welk type gegevens het betreft; aantal en categorie(en) van betrokkenen;
- mogelijke gevolgen; getroffen maatregelen om de inbreuk aan te pakken en verdere incidenten te voorkomen;
- de melding aan de betrokkenen (indien van toepassing);
- of de melding ook aan toezichthouders in andere EU-landen is gedaan;
- of de melding compleet is of dat er nog een aanvullende melding op dit incident komt.

De kennisgeving aan de AP moet tevens beschrijven:
- of de verantwoordelijke het incident aan betrokkenen zal melden, met een onderbouwing van de gemaakte keuze;
- de geconstateerde en vermoedelijke gevolgen van de inbreuk op de verwerking van de persoonsgegevens;
- welke maatregelen de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

Indien de verantwoordelijke tevens de betrokkenen inlicht, dan stelt hij hen in kennis van de mogelijke gevolgen van de inbreuk voor hun persoonlijke levenssfeer en adviseert hij over de door hen te nemen maatregelen ter beperking van schade. De kennisgeving aan de AP en de betrokkenen omvat:
- de aard van de inbreuk;
- de instantie(s) waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

Zoals al even aangestipt geldt de meldplicht *niet* indien de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn gemaakt door technische en/of organisatorische maatregelen. Maar technische anonimisering, bijvoorbeeld door versleuteling, biedt geen absolute vrijwaring: de geschatte levensduur

van de gebruikte encryptiemethode en de aard van de gegevens in kwestie moeten hierbij worden meegewogen.

Ten slotte: behalve voor het niet melden kan de AP ook boetes opleggen voor verwijtbare schendingen van meer algemene verplichtingen die de Wbp stelt aan het verwerken van persoonsgegevens, dus zonder dat er sprake is geweest van een datalek. Denk aan het onvoldoende op orde hebben van de informatiebeveiliging of de privacybescherming. Deze boete kan oplopen tot € 820.000 of 10% van de netto-omzet bedragen.

Begin 2016 is het voorstel *Wet gegevensverwerking en meldplicht cybersecurity* naar de Tweede kamer gezonden[5]. Hoewel de term gegevensverwerking in de titel gemakkelijk anders doet vermoeden, betreft het hier geen privacywetgeving. Per saldo kan het resultaat zijn dat twee meldingen bij twee, voor financiële instellingen mogelijk soms zelfs bij drie verschillende instanties moeten worden gedaan, indien door een inbreuk ook persoonsgegevens worden geraakt [6].
De reden om het voorstel hier kort in een bijlage (Bijlage 1) te bespreken is erin gelegen dat ook hier een meldplicht in het spel is die bovendien procedureel en organisatorisch veel gelijkenissen vertoont met de protocollen die nodig zijn voor de meldplicht datalekken. De wet moet gaan gelden voor bij Algemene Maatregel van Bestuur nog aan te wijzen organisaties in 'vitale sectoren'. Inbreuken zouden moeten worden gemeld aan het Nationaal Cyber Security Centrum (NCSC). Boetes bij nalatigheid lijken hierbij vooralsnog niet aan de orde.

Op 25 mei van dit jaar (2016) is de *Algemene verordening gegevensbescherming* in werking getreden in alle lidstaten van de Europese Unie. Daarmee start eerst een 'boetevrije' implementatietermijn van 2 jaar, waarin de AVG weliswaar van kracht is, maar overtredingen nog niet beboet kunnen worden. Ingezetenen van de EU kunnen zich er echter al wel op beroepen - hetgeen op zijn minst publicitaire risico's voor organisaties met zich mee kan brengen. Op 25 mei 2018 treedt overal in de EU het handhavingsregime in werking en zullen overtredingen tegen de verordening beboetbaar zijn.

Het is onmiskenbaar dat zowel de meldplicht datalekken als het voorstel Gegevensverwerking en meldplicht cybersecurity zijn ontwikkeld met het oog op het gedachtegoed op Europees niveau. Uitgebreide bespreking van de AVG en andere relevante Europese voorstellen zoals de NIB gaan buiten het bestek van deze publicatie; zij komen summier aan de orde in Bijlage 2.

[5] https://www.rijksoverheid.nl/regering/inhoud/bewindspersonen/klaas-dijkhoff/documenten/kamerstukken/2016/01/21/tk-nader-rapport-inzake-wet-gegevensverwerking-en-meldplicht-cybersecurity
[6] AP, AFM en mogelijk ook NCSC; zie ook de laatste paragraaf van Bijlage 1 op pagina 29.

3. De meldplicht datalekken

De Meldplicht datalekken is geen aparte wet, maar een uitbreiding van de Wbp met artikel 34a en aanpassing van enkele bestaande artikelen, waaronder artikel 66 over boetes[7]. De wet is gericht op "het voorkomen van datalekken ten gevolge van doorbreking van beveiligingsmaatregelen en als deze zich toch voordoen, de gevolgen ervan voor de betrokkenen zoveel mogelijk te beperken. Met de meldplicht wordt bijgedragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens"[8].

De meldplicht adresseert de 'verantwoordelijke(n) voor de verwerking van persoonsgegevens', geheel in lijn met de artikelen 1, sub d, en 15 van de Wbp. De verantwoordelijke kan een natuurlijke persoon of rechtspersoon zijn en kan deel uitmaken van de publieke of de private sector.
Hoe de meldplicht precies gehandhaafd gaat worden is nog niet helemaal duidelijk. Een houvast hiervoor is te vinden in de Beleidsregels van de Autoriteit Persoonsgegevens[9].De uitvoering van de meldplicht berust evenwel ook op een reeks van beoordelingen en interpretaties die in de eerste plaats moeten worden gemaakt door de eerder genoemde verantwoordelijke voor de gegevensverwerking zelf: is er sprake van een lek en geven de ernst resp. de (vermoedelijke) gevolgen aanleiding om bij de AP en eventueel de betrokkene(n) te melden? Daar komt bij dat een datalek niet altijd een lek hoeft te zijn in de zin van 'verlies' of 'in verkeerde handen geraakt'. Het gehanteerde begrip datalek kan ook slaan op een tekortkoming in de verwerking van persoonsgegevens, waardoor mogelijk nadelige gevolgen voor de betrokkene(n) kunnen ontstaan. Dit komt verderop nog uitgebreid ter sprake.

De AP kan per 1 januari 2016 organisaties, ook als er geen sprake is van een concreet datalek, beboeten "*bij schending van meer algemene verplichtingen die de Wbp stelt aan gebruik en verwerking van persoonsgegevens. Bijvoorbeeld als persoonsgegevens niet op een behoorlijke en zorgvuldige manier zijn verwerkt of langer worden bewaard dan noodzakelijk is, maar ook als de beveiliging niet deugt, het beheer van persoonsgegevens slecht is georganiseerd of gevoelige informatie over burgers zoals hun politieke voorkeur of levensovertuiging is misbruikt*"[10]. Deze zaken zullen eveneens een rol gaan spelen bij de beoordeling van een datalek: in hoeverre is de organisatie verwijtbaar in gebreke gebleven, waardoor de schade als gevolg van het lek groter is dan redelijkerwijze had gehoeven?

3.1 Reikwijdte

Er is pas sprake van een meldplicht voor een datalek als er een datalek is. Dat klinkt kinderachtig, maar het blijkt toch nog een hele toer om te omschrijven wanneer dat, in de zin van de wet, het geval is: als de organisatorische en/of technische beveiligingsmaatregelen niet hebben gefunctioneerd en een inbreuk op de beveiliging, als bedoeld in artikel 13 Wbp, ernstige nadelige gevolgen heeft of kan hebben voor de bescherming van verwerkte persoonsgegevens. Inbreuken op de beveiliging vinden tegenwoordig veelal plaats in digitale vorm, maar ook diefstal van papieren gegevens of het lekken via mondelinge dan wel telefonische communicatie zullen in principe onder de meldplicht vallen.

[7] Wet meldplicht datalekken en uitbreiding boetebevoegdheid cbp stb-2015-2-2. Voluit: Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp).
[8] Memorie van Toelichting, Algemeen, paragraaf 1.
[9] Voluit: De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). Beleidsregels voor toepassing van artikel 34a van de Wbp. Autoriteit Persoonsgegevens, 8 dec 2015. Wij verwijzen ernaar met 'De Beleidsregels (van de AP)'.
[10] Nieuwsbericht Meldplicht datalekken en uitbreiding boetebevoegdheid Cbp 1 januari 2016 van kracht d.d. 10-07-2015.

De AVG doet, in tegenstelling tot de nieuwe WBP-artikelen, een poging tot nadere definitie van wat daar "personal data breach" wordt genoemd: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. De vijf 'verschijningsvormen' van een datalek die in deze definitie worden genoemd komen nog uitgebreid aan de orde. Formeel wordt deze definitie als zodanig pas van kracht in de loop van 2018, na afloop van de implementatietermijn van de AVG.

Er hoeft niet noodzakelijkerwijze sprake te zijn van *verwijtbaar* onvoldoende beveiligingsmaatregelen: de beveiliging kan op orde zijn en niettemin worden teniet gedaan of omzeild. Toerekenbaar tekortschieten kan variëren van een niet adequate en niet vakkundig toegepaste beveiliging tot 'ongelukken' door bijvoorbeeld menselijke fouten.

Bij de beoordeling of er sprake is van ernstige nadelige gevolgen voor de bescherming van de desbetreffende persoonsgegevens zijn van belang:

- de aard en omvang van de inbreuk;
- de aard van de gelekte persoonsgegevens en:
- de mate waarin organisatorische en technische beschermingsmaatregelen zijn getroffen ten aanzien van de persoonsgegevens.

Bij "de aard van de persoonsgegevens" valt te denken aan gevoelige informatie waartoe bijvoorbeeld ook medische en strafrechtelijke gegevens behoren. Maar het onderliggende criterium is eigenlijk de mate van privacyschending, beschadiging of hinder die zou kunnen optreden als gevolg van de inbreuk, ook als het gegevens betreft die niet tot het bekende rijtje gevoelige gegevens cf. art.16 Wbp behoren. Dit mag naar ons idee worden geconcludeerd uit de bepaling dat de verantwoordelijke de betrokkenen onverwijld in kennis moet stellen van een inbreuk als die waarschijnlijk ongunstige gevolgen zal hebben voor hun persoonlijke levenssfeer.

De meldplicht geldt *niet* indien de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor wie geen recht heeft op kennisname van de gegevens. Het voorbeeld dat hierbij doorgaans wordt aangehaald is het verlies van een volledig versleutelde laptop. Maar pas op: met name encryptie is aan erosie onderhevig en kan mettertijd aanmerkelijk verzwakken. Daarbij kan het ook gebeuren dat de aard van de gegevens die in het spel zijn zodanig gevoelig is, dat het ondanks de versleuteling toch wenselijk is de inbreuk te melden aan de AP en de betrokkenen te adviseren over maatregelen ter bescherming van hun privacy.

De wettelijke meldplicht geldt eveneens *niet* wanneer voorzieningen van algemene aard, dat wil zeggen: die niet specifiek zijn gericht op de beveiliging (of bescherming) van persoonsgegevens, worden aangetast. Als bijvoorbeeld een blikseminslag tot gevolg heeft dat het gebouw afbrandt, waarbij ook persoonsgegevens verloren gaan, dan zal in de betekenis van de wet niet van een inbreuk op de beveiligingsmaatregelen kunnen worden gesproken (MvT, paragraaf 3.1). Merk op dat toepassing van een ruimer begrip 'beschermingsmaatregelen' hier wellicht tot wat minder stelligheid zou moeten leiden. Behoren brandpreventiemaatregelen en bliksemafleiding in dit verband tot de bescherming van persoonsgegevens? Wij kunnen ons overigens ook voorstellen dat bij een calamiteit persoonsgegevens verloren gaan in omstandigheden die het mogelijk of waarschijnlijk maken dat zij in verkeerde handen kunnen vallen.

Er zijn meer en oudere meldplichten dan de onderhavige meldplicht datalekken. Twee prominente meldplichten betreffen organisaties in de telecomsector en de financiële sector. Artikel 34a adresseert deze in lid 8 en 9:

> *8. Dit artikel [de meldplicht -red.] is niet van toepassing indien de verantwoordelijke in zijn hoedanigheid als aanbieder van een openbare elektronische communicatiedienst een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet.*
> *9. Het tweede en zevende lid* [van de meldplicht -red.] *zijn niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht.*

Hier zou het misverstand kunnen ontstaan dat het melden van datalekken aan de AP niet van toepassing is op de telecomsector. Het is echter juist het genoemde artikel 11.3a van de Telecommunicatiewet dat nu deze verplichting regelt wanneer er persoonsgegevens in het spel zijn. Telecomorganisaties zijn dus verplicht op grond van de *Telecommunicatiewet* de melding te doen *bij de AP*. Dat gedaan hebbend zijn zij niet meer gehouden de melding (nogmaals) te doen op grond van de Wbp[11].

De verplichting om datalekken te melden bij de AP is ook van toepassing op de financiële sector, maar: een financiële onderneming wordt niet verplicht om datalekken te melden *aan betrokkenen* (cf. lid.2). Dit is in lijn met de staande praktijk dat een financiële onderneming incidenten wel moet melden aan de financieel toezichthouder, maar niet aan betrokkene. Openbare kennisgevingen aan betrokkenen worden in de financiële sector als te risicovol beschouwd om dit dwingend voor te schrijven. De zorgplicht van de financiële onderneming moet waarborgen dat zij ook zonder deze verplichting haar verantwoordelijkheid jegens cliënten in rechtstreeks contact met die cliënten zal nemen. Merk op dat (ook) melden bij de AP zal kunnen leiden tot dubbel melden[12].

De relevante passages uit de Mvt over deze twee sectorale meldplichten hierover staan in Bijlage 3.
Zie over mogelijke samenloop van meldplichten ook de laatste paragraaf van Bijlage 1 op pagina **Fout! Bladwijzer niet gedefinieerd.**.

3.2 Het brede begrip 'datalek'

Volgens de wet hoeft een datalek niet noodzakelijkerwijze te betekenen dat persoonsgegevens verdwijnen of informatie daadwerkelijk weglekt zoals we "lekken" in het dagelijks leven verstaan bij een lekke band of een lekke waterleiding. Lekken betekent vaak dat je het weggelekte kwijtraakt. Daar hoeft in het geval van datalekken niet altijd sprake van te zijn. Het schenden van de vertrouwelijkheid kan ook zonder daadwerkelijk verlies van de gegevens c.q. informatie gebeuren. Iemand die afluistert bijvoorbeeld steelt weliswaar informatie, maar er treedt geen materieel verlies op. Bovendien hoeft het ook niet per se een schending van de vertrouwelijkheid te betreffen. Onbeschikbaarheid en verlies van integriteit van gegevens kunnen daar eveneens onder gerekend worden.

Ongeoorloofde of onbedoelde openbaarmaking van (persoons)gegevens zijn in feite inbreuken op de gegevensbescherming. De Wbp spreekt dan van 'onrechtmatige verwerking'. In de context van informatiebeveiliging wordt ook wel het begrip 'ongeoorloofde toegang' gebruikt, om aan te geven dat gegevens toegankelijk zijn of zijn geweest voor onbevoegden. Dit kan het gevolg zijn van een intentionele inbreuk op de beveiliging door een onbevoegde, maar ook van nalatigheid of een zwakke bescherming door de verantwoordelijke of bewerker.

[11] Er kunnen zich situaties voordoen waarin dit ingewikkelder is dan hier weergegeven. Organisaties die vallen onder de Telecommunicatiewet doen er verstandig aan de Beleidsregels van de AP goed te bestuderen, met name het beslisschema in de eerste paragraaf van hoofdstuk 4.
[12] Mvt nr 3 herdruk, par. 4.2: "Deze dubbele meldplicht zal alleen bestaan als een datalek eveneens een incident is; alsdan moet zowel aan het Cbp als aan DNB of de AFM worden gemeld." (kst-33662-3-n1).

Ongeoorloofde toegang c.q. openbaarmaking kan ook het gevolg zijn van slordig of opzettelijk foutief handelen van gegevensverwerkend personeel. Maar let op: opzettelijk ongeoorloofd handelen met persoonsgegevens waartoe op rechtmatige wijze toegang werd verkregen door toegangsbevoegden, *dus binnen ongeschonden organisatorische en technische beveiligingsmaatregelen*, geldt als misbruik. Dit kan tot ongunstige gevolgen leiden voor de persoonlijke levenssfeer van betrokkenen, maar is *niet een datalek waarop de meldplicht ziet*[13]. Wij vinden deze beperking van de reikwijdte opvallend omdat de centrale gedachte onder de meldplichtwetgeving nu juist de verbetering van de positie van betrokkenen annex bescherming van betrokkenen tegen schade is geweest. En de kans daarop lijkt ons in dergelijke gevallen van misbruik net zo aanwezig als bij datalekken.

Datalekken in de - je zou bijna zeggen - traditionele zin van het woord zijn natuurlijk de diefstal van gegevens of het kwijtraken van mobiele gegevensdragers. En zoals het kan voorkomen dat alleen de *vertrouwelijkheid* geschonden is, zo kan het ook gebeuren dat je er materieel niet meer bij kunt, of dat nu komt door diefstal, manipulatie of door een fout[14]. In zekere zin treedt die toestand ook op bij *onbeschikbaarheid* - al dan niet tijdelijk - van gegevens. Het onbeschikbaar maken van gegevens, waarna 'losgeld' moet worden betaald, is momenteel een van de meer populaire vormen van geld verdienen door het plegen van een inbreuk - niet iedereen heeft immers actuele datakopieën bij de hand. Bedenk overigens dat hierbij eveneens de vertrouwelijkheid als gecompromitteerd moet worden beschouwd - en dan moet dus behalve aan de AP ook een melding aan betrokkenen worden overwogen. Dat laatste is mogelijk niet nodig wanneer het uitsluitend een technische storing is geweest die geen gevolgen heeft voor de vertrouwelijkheid - een duidelijk geval is vooralsnog de doorgestoken datakabel of - indien de databaseprotocollen op orde zijn - een stroomonderbreking [15].

Gegevens die er in bepaalde situaties toe doen moeten niet alleen beschikbaar zijn, maar ook correct. Evenals gegevens die op kritieke momenten niet toegankelijk zijn, kunnen ook foutieve gegevens tot ernstig nadeel leiden. Het evidente voorbeeld hierbij is de dringende behoefte aan medische gegevens als het erom spant. Die moeten beschikbaar en betrouwbaar zijn. En zo zijn we aangekomen bij de schending van de integriteit van gegevens als derde invulling van het begrip 'datalek'. Foutieve gegevens worden misschien bij eerste gebruik - hopelijk niet in een noodsituatie - ontdekt en gecorrigeerd; maar als de foutsituatie al enige tijd bestaat moet je je afvragen bij wie of welke instantie(s) de verkeerde informatie ondertussen terecht gekomen en verwerkt is. Met name het doorgeven van gegevens in ketens en het toenemende gebruik van 'big data' voor analyse en 'profiling' kan dan in de toekomst nog voor onverwachte verrassingen zorgen. Denk dus niet zomaar dat een simpele correctie in de eigen administratie voldoende is om de kans op schade voor betrokkene te neutraliseren, maar ga altijd zorgvuldig na of en bij wie gemeld moet worden.

3.3 Niet alles registreren, of toch?

De aanvankelijk voorgestelde verplichting om binnen de organisatie een overzicht bij te houden van *alle* inbreuken, is in de Nota van wijziging van 15 april 2014 komen te vervallen als "minder wenselijk". Dit zou immers ook van toepassing zijn geweest op niet- of mogelijk niet-meldplichtige inbreuken, terwijl de verantwoordelijke krachtens de verplichting van Art. 13 Wbp toch al procedures ingesteld moet hebben

[13] MvT, paragraaf 3.1: "Er is dan geen sprake van het inbreuk maken op beveiligingsmaatregelen, maar het misbruik maken van vertrouwen. Hoe schadelijk dit ook kan zijn, dat is niet het onderwerp van dit wetsvoorstel" (kst-33662-3-n1).
[14] Lees - bijvoorbeeld - respectievelijk: door hacking, door ransomware of door het doorsteken van een datakabel tijdens graafwerk.
[15] We moeten in het midden laten of onbeschikbaarheid van gegevens, die niet wordt opgemerkt omdat de betreffende gegevens tijdens de onbeschikbaarheid niet worden verwerkt of gebruikt, ook onder de meldplicht valt.

voor het tijdig en doeltreffend behandelen van beveiligingsincidenten en het aanbrengen van maatregelen ter voorkoming van herhaling.

Niettemin staat de verplichting om een overzicht bij te houden "van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens" letterlijk in de wet[16]. En weet die kans maar eens van te voren… Het is juist daarom zeer de vraag of het verstandig is om géén register bij te houden. De verantwoordelijke zal hierop immers moeten kunnen terugvallen indien de AP opheldering vraagt over een beveiligingsincident. Incidentgegevens moeten minimaal één en in sommige gevallen minimaal drie jaar bewaard worden[17].
Denk hierbij ook aan toepassing van de Wet openbaarheid van bestuur (WOB) en mogelijk ook de Archiefwet. Hou daarom hoe dan ook rekening met de invoering van een administratie van incidenten.

> *In januari 2016 werd de vraag gesteld of iedere SQL-injectie-kwetsbaarheid, die door een ethische hacker wordt gevonden in een portal waar gevoelige persoonsgegevens worden verwerkt, aan de betrokkene gemeld dient te worden, tenzij kan worden aangetoond dat hiervan geen misbruik is gemaakt. Dat zou nogal wat consequenties hebben voor de praktijk*[18].
> *In oktober 2016 wordt in een artikel gesteld dat het niet melden van cybercrime (waarmee hier ook een datalek is bedoeld -red.) vaak verstandiger is dan wel melden. Hij betoogt dat de kans op imago- en vervolgschade vele malen groter is dan de kans op vervolging. Dit artikel heeft de Tweede Kamer gehaald*[19].
> *Het kan wellicht ook anders. De Nederlandse beroepsorganisatie voor IT-auditors (NOREA) acht een jaarlijkse bestuursverklaring over datalekken wenselijk met het oog op de controleerbaarheid van de meldplicht. De RvB zou jaarlijks expliciet moeten verklaren dat er geen datalekken zijn vastgesteld. De wetgever heeft dit voorstel niet overgenomen, maar het is denkbaar dat een dergelijke maatregel, onder meer door de komst van de AVG, zijn weg gaat vinden naar de diverse normenkaders en de auditpraktijk. Tegelijkertijd is het met de ruime definitie van 'datalek' onwaarschijnlijk dat zich in enig jaar geen datalekken zullen voordoen.*

3.4 Beslismodel meldplicht Wbp: "melden indien"

De goede werking en het succes van de wet hangen erg af van hoe men omgaat met de risico-inschattingen die op de beslismomenten moeten worden gemaakt. Zoals hierboven gezegd gaat het om inbreuken die 'ernstige nadelige gevolgen' hebben voor de bescherming van de verwerkte persoonsgegevens. In die gevallen spreek je van een datalek. Ernstige datalekken moeten bij de AP worden gemeld. Betrokkenen moeten worden ingelicht indien het 'waarschijnlijk' is dat er 'ongunstige gevolgen' zullen zijn voor 'hun persoonlijke levenssfeer'.

> *De AVG hanteert overigens de omgekeerde aanvliegroute: "melden tenzij" de verwerkings-verantwoordelijke kan aantonen dat het onwaarschijnlijk is dat een inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt.*

[16] Artikel 34a, lid 8: "De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene".
[17] "De wet schrijft niet voor hoe lang u het overzicht moet bewaren. Ga uit van een bewaartermijn van minimaal een jaar. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren" Bron: De Beleidsregels van de AP, pagina 46. Zie hierover ook: Mark Janssen Valkuil onder komend privacyrecht (15 juni 2016).
[18] Advocaat Huub de Jong in "Klaar voor een datalek", Madison Gurkha, januari 2016.
[19] Advocaat Aldo Verbruggen in artikelen van Rob de Lange in het Financieel Dagblad, 24 oktober 2016 "Melden van cybercrime zou bijdragen aan het algemeen belang. Ik betwijfel dat zeer" en "Niet melden cybercrime is vaak verstandiger".

1	Datalek?	Is er sprake is van een inbreuk op de getroffen beveiligingsmaatregelen die *ernstige nadelige gevolgen* heeft voor de bescherming van verwerkte persoonsgegevens. Hieronder valt ook de inschatting of eventueel getroffen technische afschermingsmaatregelen, bijvoorbeeld door encryptie van de inhoud of het toepassen van het op afstand wissen van de inhoud of onklaar maken van de drager ('remote wipe'), voldoende robuust en tijdig zijn om ongeoorloofde toegang met zekerheid uit te sluiten; e.e.a. afgezet tegen de aard van de gegevens in kwestie.
2	Betrokkenen?	Is het waarschijnlijk dat de inbreuk voor de persoonlijke levenssfeer van de betrokkenen *ongunstige gevolgen* zal hebben? Hiervoor is een kwalitatieve evaluatie van de bij een datalek betrokken gegevens nodig, alsook de mogelijke betekenis ervan voor de betrokkenen. Zonodig moet deze evaluatie ook buiten de grenzen van de eigen verwerking plaatsvinden en zich uitstrekken tot direct aan de verwerking gelieerde ketenpartners en verdere verwerkers.

Fig.1

Beide vragen vergen van de verantwoordelijke een beslissing die niet altijd of soms maar ten dele is gebaseerd op harde gegevens of algemeen aanvaardbare inschattingen. In de MvT wordt de verwachting verwoord dat het CBP nog met nadere richtsnoeren voor de uitvoering zal komen ten behoeve van "indirect enig houvast" voor de praktijk[20]. De AP heeft vervolgens in de Beleidsregels voor toepassing van artikel 34a van de Wbp, onder meer in paragraaf 4.2.2., inderdaad een aantal aanwijzingen neergezet, maar geen harde criteria.

3.5 Schema voor de afwikkeling van incidenten

Figuur 2 geeft in grote trekken aan hoe de organisatie met het beslismodel van de nieuwe wet zou kunnen omgaan. De twee vragen verwijzen naar Fig.1 in paragraaf 3.4.

Een 'incident' is een inbreuk op de beveiliging; dit wordt een 'datalek' als er persoonsgegevens bij verloren zijn gegaan die het qua aard of hoeveelheid een ernstig incident maken en niet kan worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt.

Aan trefzekere werking van dit beslismodel gaan niet te onderschatten randvoorwaarden vooraf. Er is acute, gedetailleerde en actuele kennis nodig van alle verwerkingen die in eigen huis of bij de bewerker(s) plaatsvinden en inzicht in de classificatie van alle verwerkte gegevens.

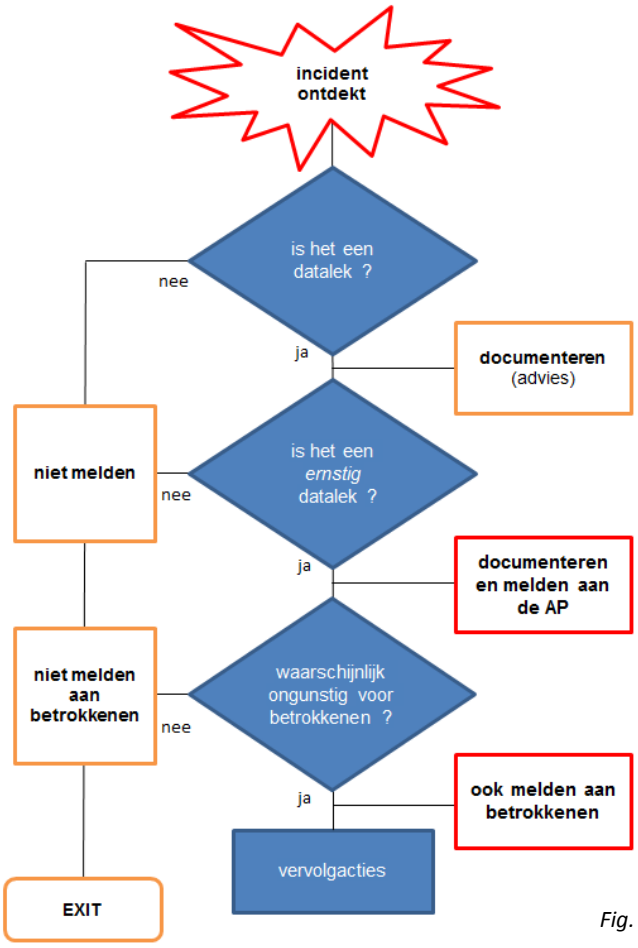

Fig. 2

[20] MvT, paragraaf 3.2.2; inmiddels is dat de AP geworden en heten de richtsnoeren 'Beleidsregels'.

Voor een goed werkend datalekprotocol zijn bovendien het actueel en bekend houden van procedures en sleutelfiguren nodig, vergelijkbaar met de protocollen voor (andere) calamiteiten. Maar een breed gedeelde 'awareness' en incident-sensitiviteit in de gehele organisatie zijn lastig te bewerkstelligen en aan slijtage onderhevig.

Zoals reeds behandeld in paragraaf 3.1, maar volledigheidshalve herhaald: voor organisaties in de financiële sector geldt de eventuele verplichting om de betrokkenen in te lichten niet, dat wil zeggen: niet uit hoofde van de Wbp. Meer hierover eveneens in het volgende hoofdstuk: "Wat moet je regelen?".

3.6 Melding

Aan de inhoud van de melding wordt een aantal eisen gesteld. De Beleidsregels geven aan dat de kennisgeving aan de AP naast de feitelijke incidentmelding, de aard en de omvang ervan ook moet ingaan op onder meer:

- het wettelijk kader voor de melding (bijvoorbeeld Wbp, Telecomwet); contactgegevens, sector;
- welk type gegevens het betreft; aantal en categorie(en) van betrokkenen;
- mogelijke gevolgen; getroffen maatregelen om de inbreuk aan te pakken en verdere incidenten te voorkomen;
- de melding aan de betrokkenen (indien van toepassing);
- of de melding ook aan toezichthouders in andere EU-landen is gedaan;
- of de melding compleet is of dat er nog een aanvullende melding op dit incident komt.

De kennisgeving aan de AP moet tevens beschrijven:

- of de verantwoordelijke het incident aan betrokkenen zal melden, met een onderbouwing van de gemaakte keuze;
- de geconstateerde en vermoedelijke gevolgen van de inbreuk op de verwerking van de persoonsgegevens;
- welke maatregelen de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

Indien de verantwoordelijke tevens de betrokkenen inlicht, dan stelt hij hen in kennis van de mogelijke gevolgen van de inbreuk voor hun persoonlijke levenssfeer en adviseert hij hen over het beperken of voorkomen van eventuele schade. De kennisgeving aan de AP en de betrokkenen omvat:

- de aard van de inbreuk;
- de instantie(s) waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

Voor de volledige opsomming van de vereiste gegevens verwijzen wij naar de Beleidsregels van de AP, pagina 51 en verder. Overigens heeft de AP bij het opstellen van de vereisten aansluiting gezocht bij (een conceptversie van) de AVG.
Wees erop bedacht dat achter dit lijstje wellicht veel meer voorbereiding schuil gaat dan het opstellen van een meldings- en afhandelingsprotocol: kén de organisatie. Zijn alle gegevensverwerkingen en hun grondslagen actueel gedocumenteerd en is een overzicht daarvan direct paraat - om maar iets te noemen. Hoofdstuk 4 gaat hier nader op in.

3.7 Verhouding 'verantwoordelijke voor de verwerking' en 'bewerker'

De wet richt zich tot de verantwoordelijke in de zin van de Wbp. Dit blijft zo wanneer een verantwoordelijke zich bedient van een bewerker. Verantwoordelijke en bewerker, doorgaans in een opdrachtgever - opdrachtnemer relatie, zullen in een *bewerkersovereenkomst*[21] afspraken moeten maken over tijdige melding van incidenten die mogelijk tot melding aan de AP en verdere acties zullen leiden. Over het belang van sluitende bewerkersovereenkomsten en het stapeleffect van mogelijke schadeclaims komen we nog te spreken in de paragrafen 4.4 t/m 4.6.

3.8 Boetes en de boetebevoegdheid van de Autoriteit Persoonsgegevens.

Het is een uitdaging om erachter te komen welke boetes de AP in welke gevallen kan opleggen. De boetebevoegdheid wordt geregeld in de artikelen 65 en 66 van de Wbp, maar dan weet je nog niets. De AP mag bestuurlijke boetes uitdelen tot een maximum van € 820.000, conform het boetemaximum van categorie 6 van het Wetboek van Strafrecht, eventueel verhoogd naar 10% van de jaaromzet als categorie 6 geen passende bestraffing toelaat. Maar tot dat bedrag hoeft het niet per se te komen.
Met een aparte uitgave, genaamd: Boetebeleidsregels Autoriteit Persoonsgegevens 2016 wil de AP inzicht geven in hoe de hoogte van een bestuurlijke boete zal worden bepaald. Maar ook daarin is het nog even puzzelen. De AP kent een eigen categorie-indeling voor boete "bandbreedtes" en hanteert daarbij andere bedragen dan het Wetboek van strafrecht in art. 23 doet [22]. Alleen de maximale standaard bovengrens van €820.000 is herkenbaar.
Uiteindelijk wordt in de bijlage duidelijk dat slechts bij één van de overtredingen in het kader van de meldplicht, te weten: *het niet-nakomen van een bindende aanwijzing*, het maximale standaard-boetebedrag van € 820.000 gehanteerd kan worden. Alle andere aan de meldplicht gerelateerde vergrijpen vallen in de categorieën I en II, en dat betekent een maximale boete van € 500.000.
Alle boetebedragen kunnen worden aangepast naar boven of naar beneden naar mate de AP meent verzachtende of verzwarende omstandigheden in aanmerking te moeten nemen, dat dan weer wel. Ook financiële omstandigheden kunnen van invloed zijn, of 'preventieve werking', en bij meerdere overtredingen kunnen de boetes worden gestapeld. In de artikelsgewijze toelichting (bij art. 6) van de Boetebeleidsregels lezen we deze passages:

> *De Autoriteit Persoonsgegevens stemt de beoordeling van de aard en omvang van de overtreding in ieder geval af op: de schaal waarop de overtreding heeft plaatsgevonden, de intensiteit van de overtreding en het stelselmatige of incidentele karakter ervan. De Autoriteit Persoonsgegevens stemt de beoordeling van de impact van de overtreding op (de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor) de betrokkenen en/of de maatschappij bijvoorbeeld af op: het (financiële) voordeel dat de overtreder heeft behaald met de overtreding en/of de schade die betrokkenen hebben geleden door de overtreding.*

Ten slotte: omdat de boetebedragen niet gelijk, maar toch wel gerelateerd zijn aan de boetecategorieën in het Wetboek van strafrecht, is het aannemelijk dat de bedragen zullen worden aangepast wanneer zij in het Wetboek worden aangepast. En dat gebeurt elke twee jaar.

[21] Verwerker/verwerking en bewerker/bewerking worden nogal eens door elkaar gebruikt, ook in combinatie met 'overeenkomst'. Op basis van de wet spreken wij van een VERANTWOORDELIJKE, een VERWERKING (van persoonsgegevens) en een BEwerker die namens een verantwoordelijke deze gegevens VERwerkt. NB: De AVG kent alleen nog maar een VERwerker ('processor') die namens een verwerkingsverantwoordelijke persoonsgegevens VERwerkt (art.4, Definities, definitie nr.8).
[22] http://www.wetboek-online.nl/wet/Sr/23.html

4. Wat moet je regelen?

Er zijn inmiddels publicaties en cursussen verschenen, er worden seminars gegeven die, soms vanuit verschillende perspectieven, ingaan op de implicaties van de meldplicht en de gevolgen voor de organisaties die met persoonsgegevens van doen hebben. Op het internet levert 'datalek' een lange lijst van hits op. Wij stippen hieronder kort een aantal relevante aspecten aan, leggen wat eigen accenten en verwijzen voor verdieping naar eerder bedoelde bronnen.

Wat je moet regelen is gemakkelijk opgeschreven: registreer en documenteer incidenten, evalueer ze en handel zo nodig. Dit lijkt *business as usual* voor organisaties die al jarenlang informatiebeveiliging moeten praktiseren volgens internationale standaarden. Toch vermoeden we dat veel van deze organisaties het nog lastig zullen vinden van de ene op de andere dag aan de meldplicht datalekken te voldoen. Terwijl we toch moeiteloos een rijtje nare (bestuurlijke) risico's kunnen opnoemen[23]:

- Reputatieschade;
- Protestacties, inmenging belangenorganisaties;
- Inmenging AP; boetes;
- Schadeclaims; afhandelingskosten
- Omzetverlies;
- Onteigening van data en processen (verlies van business);
- Innovatieremmer;
- Verlies van klanten;
- Ontslagen, verlies van banen;
- Faillissement;
- Gerechtelijke vervolging.

Een deugdelijk aanvals- c.q. verdedigingsplan kent deze twee pijlers:
1. Preventie en detectie: organiseer kennis en ontwikkel awareness;
2. Reactie en afhandeling: organiseer oefening en ontwikkel routine(s).

In de volgende paragrafen lichten we hiervan een aantal aspecten uit.

4.1 Ken de organisatie en de business

Het is zo basaal dat je er wellicht juist niet aan denkt. Kijk weer eens goed naar de organisatie met het oog op de nieuwe wetgeving: weten we (exact!) welke gegevensverwerkingen we doen, hebben we er beleid voor opgeschreven en geaccordeerd, wat zijn de risico's, wie in de organisatie gaan erover, is er controle, zijn bewerkersovereenkomsten juridisch correct en voldoende, wie zijn onze directe ketenpartners (leveranciers, afnemers), etc. Deze zaken lijken evident, maar kan de organisatie deze informatie binnen de gestelde termijn van 72 uur - of überhaupt wel - actueel en compleet opleveren?

Eigenlijk zou je dat als organisatie ook los van de meldplicht en een eventueel datalekincident paraat moeten hebben om transparant te kunnen zijn over hoe de organisatie de privacy van klanten c.q. betrokkenen waarborgt en welke efficiencykeuzes daarbij eventueel worden gemaakt. Als kwaliteit van dienstverlening en marketing hiervoor geen goede redenen waren in deze tijd van groeiende (maatschappelijke) aandacht voor privacy, dan is er nu ook de AVG om (lakse) organisaties bij de les te brengen.

[23] Vrij naar een presentatie voor CIP door Sergej Katus van Privacy Management Partners (maart 2014).

Uit het aanbod op internet geven we hier een van de modellen voor een methodische aanpak, gevonden in een programmafolder over voorbereiding op de nieuwe wetgeving[24].
Loop bijvoorbeeld in figuur 3 hieronder de paarse vlakken op de tweede rij eens na in het licht van de meldplicht, en eigenlijk ook al de AVG.

Fig.3

Een aantal van deze aspecten komt hierna aan de orde, niet alleen in het kader van governance, verantwoordelijkheden en boetes, maar ook in het licht van aansprakelijkheid en mogelijke schadeclaims.
Hoe ver is de organisatie op deze punten, wat moet er nog gebeuren en in welke volgorde? Organiseer de noodzakelijke kennis en pak de lacunes aan.

4.2 Implementeer en maak aantoonbaar

De organisatie moet aantoonbaar(!) maatregelen hebben getroffen die:
- de frequentie van beveiligingsincidenten laag houden;
- de ontdekkingskans groot maken;
- zorgen voor een efficiënte afwikkeling van incidenten;
- leiden tot leren en verbeteren.

De realisatie hiervan zal per organisatie verschillen als gevolg van organisatiecomplexiteit en keuzes naar aanleiding van risico-inschattingen. Het raamwerk in figuur 4 op de volgende pagina biedt richting en focus bij het bedenken van wat er zoal moet gebeuren.

[24] Fig.3 is met toestemming overgenomen van SeByde BV.

Per vakje kun je invullen wat ervoor nodig is en in hoeverre de organisatie dat gereed en bij de hand heeft[25].

Merk op dat je naast de AP en betrokkenen mogelijk ook ketenpartners op de hoogte moet stellen van een datalek ("meld overige partijen").

Over aantoonbaarheid nog dit: een datalek kan iedere organisatie overkomen. Maar je moet het melden en dat betekent dat je de aandacht van de toezichthouder op je vestigt. Deze verwacht binnen de gestelde termijn de vereiste informatie op zijn bureau hebben. Gestuntel daarmee is dan op zijn minst niet handig.

Fig. 4

4.3 Risico's minimaliseren

Veruit de grootste maar ook nuttigste inspanning tegen datalekken zijn maatregelen die risico's minimaliseren. Minimaliseren is iets dat de gehele organisatie aangaat en ook bij detectie zijn idealiter alle onderdelen betrokken.

Het meeste werk zit in de alledaagse gang van zaken. Daarin moeten de voorwaarden verweven zitten die preventief werken en die de kans op datalekken minimaliseren. Onderscheid naar verschillende oorzaken van datalekken geeft een idee van waar en hoe preventie moet worden ingeregeld.
Voor de gelegenheid, en zonder dat we er een uitgebreide studie naar hebben gedaan, onderscheiden we als het om preventie gaat de volgende drie datalek-risicogebieden.

1. "materiele" datalekken: verloren datadragers als usb sticks en laptops, maar ook weggegooide ordners, mobiele telefoons - al dan niet 'van de zaak', kortom: gegevensdragers die verloren raken of gestolen worden. Eigenlijk de gemakkelijkste categorie: het betreft 'dingen' die zoek zijn. In principe snel te ontdekken en goed te duiden. Behalve gerichte acties en maatregelen is de hoofdzaak 'zorgvuldig handelen'. Of medewerkers die het overkomt (kwijtraken) dit ook gemakkelijk zullen melden is een andere kwestie die de nodige aandacht verdient.
2. "mondelinge datalekken", bijvoorbeeld loslippigheid bij vergissing, niet in de gaten hebben dat wordt meegekeken of meegeluisterd (in de trein, in openbare ruimtes), en bewuste mondelinge overdracht van vertrouwelijke informatie aan derden die er geen recht op hebben. Behalve bevorderen dat medewerkers zorgvuldig en bewust met hun werk omgaan is er weinig aan - of tegen te doen. Een gemeenschappelijk normbesef en sociale controle op de werkvloer bieden wellicht nog de beste resultaten.

[25] Vrij naar een schema dat is gepresenteerd door Joris Hutter van Privacy Management Partners op 6 oktober 2015 (Lantech event Meldplicht Datalekken).

3. "datalekken in cyberspace": wie een betere term weet mag het zeggen. We bedoelen de niet-materiële datalekken, in contrast tot de 'materiële'. Misschien dekt de term 'softwarelekken' de lading ook: je raakt geen spullen kwijt, wel informatie. Ingeprogrammeerde achterdeurtjes in de database, slordig programmeerwerk, slecht geteste releases, slordig beheer (patchmanagement!), onvoldoende beveiligingsmaatregelen, verkeerde instellingen, lek door toedoen van hacking, … Hieronder vallen in ieder geval ook de eerder besproken situaties van onbeschikbaarheid en corruptie van gegevens.

Het vermelden van grote aantallen e-mailadressen per ongeluk in de Aan in plaats van de BCC is qua indeling een twijfelgeval, maar dat is minder van belang. Het is ondoordacht handelen door IT-gebruikers. Er zijn IT-oplossingen voor om deze vorm van onzorgvuldigheid tegen te gaan.
Minimalisatie en de kans op detectie liggen voor de eerste twee categorieën dicht bij elkaar. Investeren in minimaliseren loont voor deze risicogebieden daarom des te meer.

Voor herstel en vervolgacties onder 3 is een meer toegespitste en vooraf goed geplande en regelmatig geoefende handelwijze nodig van een vooraf geformeerd gelegenheidsteam dat meteen beschikbaar en operationeel is wanneer nodig, vergelijkbaar aan de escalatieprocedures en organisatie in geval van calamiteiten.

Het kan gebeuren dat inbreuken pas lang nadat ze hebben plaatsgevonden aan het licht komen. Slimme hackers hebben geduld en doen er alles aan om de ontdekking zo lang mogelijk voor te zijn. Zij creëren daarmee een langdurig datalek, of in ieder geval de mogelijkheid daarvoor.
Een hack hoeft echter niet altijd de oorzaak te zijn. Onzorgvuldig beheer of slordig geprogrammeerde applicaties kunnen structurele datalekken veroorzaken. Dergelijke hacks en lekken kunnen al dan niet vroegtijdig worden ontdekt door pentesten, ethical hacking, code review. Secure software development is de aangewezen weg om het risico op softwarefouten te minimaliseren. In dit kader kun je (moet je) al heel wat huiswerk doen vóórdat je te maken krijgt met een datalek. Deze voorbereidingen en preventieve maatregelen zijn evident nuttig en nodig om te minimaliseren, maar zij verhogen ook awareness en maken het mogelijk om slagvaardig te kunnen zijn als het erop aan komt en een goede indruk te maken op de toezichthouder als die vragen komt stellen over een incident.
Maar de eerste en alledaagse maatregel voor categorie 3 is: *hou logfiles bij en doe er iets mee*.

4.4 Organiseer accountability

De kernbegrippen in de melding-datalek-problematiek zijn:
- Incident'sensitiviteit' op orde;
- Breed gedeeld besef van het belang van incidentmeldingen;
- Verantwoordelijkheden belegd, juridische dekking;
- Beveiliging op orde (human & tech);
- Administratie- en controleroutines op orde;
- Maatregelen voor detectie, damage control en herstel;
- Slagvaardigheid/tijdigheid;
- Inschattingen van schade;
- Gemotiveerde kennisgeving aan de AP;
- Kennisgeving & advies aan betrokkene(n);
- Rapportage/registratie;
- Feedbackverwerking;
- Beperking/herstel imagoschade.

Op deze punten zal de organisatie voldoende in control, actief, voldoende robuust en voorbereid moeten zijn en slagvaardigheid van handelen moeten hebben. Niet alleen nadat een incident heeft plaatsgehad, maar ook al ver daaraan voorafgaand. Dat moet niet alleen uit het oogpunt van goede dienstverlening, compliancy[26] en uit respect voor de klant wiens gegevens in vertrouwen zijn afgegeven, het is ook zeer aan te raden uit het oogpunt van accountability en mogelijke ingebrekestelling. Met de komst van de AVG komt ook hoofdelijke aansprakelijkheid in ketens als prominente risico in beeld. Artikel 82 van de AVG behandelt het recht op schadevergoeding en aansprakelijkheid. Het bouwt voort op artikel 23 van Richtlijn 95/46/EG, breidt dit recht uit tot schade die is veroorzaakt door verwerkers en verduidelijkt de aansprakelijkheid van gezamenlijk voor de verwerking verantwoordelijken en gezamenlijk opererende verwerkers[27]. Een dergelijke aansprakelijkheid is overigens niet nieuw: ook onder de Wbp (Art. 49 lid 3) bestaat deze.

Het op orde brengen van een informatiepositie kan een hele klus zijn; de administratie alleen al:

- Is er adequate, actuele informatie paraat over elke(!) gegevensverwerking?
- Zijn de verantwoordelijkheden correct, expliciet en sluitend belegd in alle(!) bewerkersovereen-komsten?
- Levert de organisatie gegevens aan of in een keten? Weet je ook dan wie de (alle!) vervolgbewerkers zijn? Je blijft immers de verantwoordelijke voor de bewerking van de gegevens die je aanlevert, ook als die weer worden doorgeleverd.

Iets breder gezien is dit allemaal informatie die tevens een rol speelt bij aantoonbaar compliant zijn. Zonder documentatie geen compliancy. Combineer dus deze zaken met de vereisten waar je toch al aan moet voldoen en (wellicht) op geaudit wordt.

Van groot belang is dat je adequate informatie paraat hebt als de AP erom vraagt en op deze punten geen risico loopt op misverstanden met bewerkers. Een op zichzelf niet zeer schadelijk datalek kán de AP ertoe brengen een onderzoek in te stellen naar de algehele status van informatiebeveiliging en privacybescherming in de organisatie. Bedenk: de toezichthouder hoeft slechts de vragen te stellen, de organisatie heeft de exhibitieplicht en moet de gevraagde bewijsstukken zonder meer overleggen[28].

4.5 Beperk vermijdbare schadeclaims

Het doen van een kennisgeving van een datalek aan de betrokkene ontheft de verantwoordelijke niet van eventuele burgerrechtelijke aansprakelijkheid voor schade die voortvloeit uit het toerekenbaar niet of niet voldoende naleven van de verplichting neergelegd in artikel 13 van de Wbp:
"*De kennisgeving aan de betrokkene is een uiting van de algemene verplichting tot schadebeperking die deel uitmaakt van het aansprakelijkheidsrecht, met inbegrip van het bijzondere aansprakelijkheidsrecht van de Wbp (art. 49). Verantwoordelijken doen er daarom goed aan dit bij de afweging om wel of geen kennisgeving aan betrokkenen te doen mee te nemen*".

[26] IBD heeft een goede 2-pager over de meldplicht en de voorbereiding daarop: Factsheet Meldplicht datalekken.
[27] Het woord 'hoofdelijk' komt in de Nederlandse vertaling van de AVG niet voor. Wel staat er in art.82 lid 2: "Elke verwerkingsverantwoordelijke die bij verwerking is betrokken, is aansprakelijk voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op deze verordening". Volgens de AVG-definitie is een verwerkingsverantwoordelijke "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt".
[28] http://www.wetboek-online.nl/wet/BW3/15i.html

Hier wordt gerefereerd aan het risico van schadeclaims wanneer onterecht geen kennisgevingen worden gedaan aan de betrokkenen met adviezen over hoe zij hun schade zouden kunnen beperken. De schades en daarmee de eventuele claims kunnen dan hoger uitvallen dan wanneer de verantwoordelijke tijdig de betrokkene zou hebben geadviseerd[29].

4.6 Maak bewerkersovereenkomsten hard

Een stevige aanrader is om de bewerkersovereenkomsten (*alle* bewerkersovereenkomsten) nog maar eens goed tegen het licht te houden in relatie tot aansprakelijkheid voor schade als gevolg van een datalek bij bewerkers of ketenorganisaties die mogelijk daardoor stil komen te vallen en/of ook op hun beurt niet door kunnen leveren. Dit betreft al snel heel wat meer organisaties dan je op het eerste gezicht zou vermoeden. Hoe het ook zij: dit is werk voor gespecialiseerde juristen, maar de verantwoordelijke moet ook hier zijn risico's kennen[30].
Op de site van de Informatie Beveiligingsdienst (IBD, www.ibdgemeenten.nl) staat een modelovereenkomst en nog wat tips en verwijzingen. Om een concrete indruk te geven van de zaken die contractueel geregeld kunnen en moeten worden komt onderstaande passage daaruit goed van pas:

"De aspecten die in een (bewerkers)overeenkomst moeten worden opgenomen en duidelijk moeten zijn:

- Wie de verantwoordelijke is en wie de bewerker is.
- Welke (soort) persoonsgegevens worden verwerkt en eventueel de wettelijke basis.
- Welke verwerkingen de bewerker precies moet doen. Hierbij kan ook geregeld worden wat de bewerker (in ieder geval) niet mag doen.
- De bewerker mag de persoonsgegevens uitsluitend bewerken in opdracht van de verantwoordelijke. De bewerker mag dus niet zelfstandig besluiten om, in afwijking van die opdracht, de persoonsgegevens op een bepaalde manier te verwerken. Tenzij een wettelijke verplichting dat vereist.
- Dat de bewerker zelfstandig aansprakelijk is voor schade die door de bewerker is veroorzaakt en hem kan worden toegerekend. En, eventueel, dat in geval de verantwoordelijke aansprakelijk gehouden wordt voor verwerkingen door de bewerker, de verantwoordelijke een regresrecht heeft (vrijwaringsbepaling).
- Dat de bewerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke dient daartoe instructies te geven, en dient toe te zien op naleving van die maatregelen.
- Wanneer een bewerker buiten de Europese Economische Ruimte (EER) gevestigd is, dient de verantwoordelijke ervoor zorg te dragen dat de bewerker het recht van het land van de verantwoordelijke nakomt (Art.14 lid 4 Wbp).
- Dat de verantwoordelijke de mogelijkheden heeft om te controleren dat de bewerker zich (geheel) aan de overeenkomst houdt. Dit kan ook worden aangetoond met bijvoorbeeld een Third Party Memorandum (TPM), waarbij de verantwoordelijke de mogelijkheid van controle heeft.
- De verantwoordelijke dient duidelijk aan de bewerker aan te geven welke maatregelen hij vereist voor het beschermen van de persoonsgegevens. (…)"

[29] De keerzijde is dat de betrokkene (een deel van de) schade mogelijk niet kan verhalen wanneer hij de aanbevelingen van de verantwoordelijke niet in acht neemt.
[30] Over financieel risico: The Ponemon Institute Fifth annual survey (2015) rekent uit dat "data breach incidents cost U.S. companies $204 *per compromised customer record* in 2009". Het tot nu toe grootste bekende lek van gevoelige data vond begin 2015 plaats bij Anthem Insurance, de #2 gezondheidszorgverzekeraar van de Verenigde staten: *78,8 miljoen bestanden*. Als Ponemon gelijk heeft was dat een schadepost van 16 miljard. Overigens lijken de kosten per record in 2016 met ongeveer 25% te zijn teruggelopen. Het gaat deze publicatie te buiten, maar het zou aardig zijn om te achterhalen of daar een aanwijsbare en te manipuleren oorzaak voor aan te wijzen is (http://www-03.ibm.com/security/data-breach/).

Wij voegen daaraan nog specifiek toe dat het verstandig, misschien wel noodzakelijk is om over de administratie van incidenten in de bewerkersovereenkomst(en) afspraken te maken die ertoe leiden dat de verantwoordelijke zijn verantwoordelijkheden jegens de toezichthouder en de betrokkenen kan waarmaken. Het lijkt ons onwaarschijnlijk dat zoiets mogelijk is zonder informatie van de bewerkers.

Wanneer bij de uitbesteding van de verwerkingen cloudaspecten moeten worden meegenomen verwijzen we, evenals IBD, graag naar de ENISA (European Union Agency for Network and Information Security), met name naar: Procure Secure: A guide to monitoring of security service levels in cloud contracts.

Wie de blik al op de (nabije) toekomst richt, doet er verstandig aan ook artikel 28 van de AVG te raadplegen: daarin staan nogal gedetailleerde aanwijzingen voor de bewerkersovereenkomst en het inschakelen van bewerkers. Los van de juridische component is het natuurlijk een goed idee om met toeleverende en afnemende partijen tot een goede verstandhouding te komen over het wat en hoe in geval van datalekken die de keten raken. Dit past vooral in het gedachtegoed van de AVG: het gaat in essentie om gedragsverandering bij de organisaties die werken met gegevens van burgers. In dit verband wijzen we ook graag op de CIP-publicatie Grip op Beveiligingsovereenkomsten - Een prestatiegerichte aanpak in beveiligingsovereenkomsten, over een andere manier van omgang tussen opdrachtgever en leverancier, teneinde een zo goed mogelijke samenwerking en een optimaal resultaat te bewerkstelligen.

4.7 Zorg voor een heldere interne procedure: een datalekprotocol

De aandacht in deze problematiek richt zich veelal gemakkelijk op de soms lastige beoordeling of een inbreuk of datalek gemeld moet worden. Maar daar gaat nog een heel organisatievraagstuk aan vooraf.

Zorg ervoor dat je niet hoeft te improviseren wanneer het feit daar is. Een *datalekprotocol* zorgt ervoor dat de juiste mensen op het juiste moment worden geïnformeerd en handelen waar nodig. Wie moeten we intern op de hoogte brengen van de inbreuk? Wie bepaalt of we het datalek moeten melden? Met welke juridische aspecten moeten we rekening houden? Indien een organisatie beschikt over een functionaris voor de gegevensbescherming kan het bijvoorbeeld voor de hand liggen om deze functionaris als beslisser aan te wijzen. Win bij twijfel deskundig advies in over de afhandeling van de melding[31].

Er moet voor ICT-incidenten mogelijk ook gespecialiseerde technische en procedurele kennis in de organisatie komen, intern dan wel ingehuurd, over wat te doen en vooral wat te laten als forensisch onderzoek aan IT-componenten wenselijk of nodig is. Het kan uiterst belangrijk zijn om apparaten aan te laten staan totdat de speurneuzen zijn gearriveerd. Er moet dus een procedure in de organisatie zijn die dat borgt als het geval zich voordoet. Dergelijke kennis is bij diverse gespecialiseerde bedrijven te verkrijgen, maar een goede instap biedt ongetwijfeld het NCSC.

4.8 Gebruik bestaande escalatiemodellen

Implementatie hoeft niet zo'n tour de force te zijn indien wordt aangesloten bij reeds bestaande business continuïteits- en calamiteitbeheersingsprotocollen. Voorwaarde is dan wel dat deze protocollen 'levend' en goed geoefend zijn. Snel en adequaat onder controle brengen en afwikkelen zal sterk verbeteren indien:

- de focus van reactief naar proactief wordt verlegd, en:
- er veel meer aandacht komt voor internalisatie bij alle medewerkers i.p.v. het treffen van uitsluitend bouwkundige of IT-gerelateerde informatiebeveiligingsmaatregelen.

[31] Voor deze passage is gebruik gemaakt van "Stap 1" in Anton Ekker - In 4 stappen voldoen aan de meldplicht datalekken.

- Uitvoering en realiteit
- Er zijn nog wel wat vragen te stellen bij de uitvoerbaarheid van de wet.
- Wat zijn we precies kwijt: dat is lang niet altijd met zekerheid vast te stellen.
- Hoe groot is de kans op misbruik als gevolg van het dataverlies?
- En hoe schatten we de kans in op "ernstige nadelige gevolgen voor de persoonlijke levenssfeer van betrokkenen"?
- Zijn de gestelde tijdvensters voor handelend optreden reëel? (bijvoorbeeld: Sony moest miljoenen gamers over de hele wereld op de hoogte stellen. Een bedrijf dat in korte tijd zonder maatregelen dergelijke aantallen e-mails de deur uit doet wordt heel snel als wereldwijde spammer aangezien en op allerlei zwarte lijsten geplaatst).
- Het wetsvoorstel eist dat "onverwijld" gemeld wordt aan de AP en de betrokkene (Wbp art. 34a). Of gelijktijdig aan de AP en de betrokkene moet worden gemeld of na elkaar, is volgens de AP afhankelijk "van de omstandigheden van het geval".
- Hoe gaat handhaving eruit zien en op welke criteria komt de nadruk te liggen?
- Wat zal, gehouden tegen de bedoeling van de wetgever[32], de invloed zijn van de mogelijkheid om de schade als gevolg van datalekken te verzekeren? Geldt dat ook bij grove nalatigheid?[33]

De Beleidsegels van de AP leren dat de in de wet ingevlochten subjectiviteit van de beoordelingen, die de verantwoordelijke moet doen om tot handelen te komen, nauwelijks tot niet door handreikingen wordt opgeheven. De AP komt niet verder dan het geven van voorbeeldgevallen. Ook over de reactie van de AP in voorkomende gevallen worden we niet veel wijzer: veel hangt alweer af "van de omstandigheden van het geval". Alleen wie willens en wetens 'apert' in de fout gaat door een meldingsplichtig incident *niet* te melden, kan zeker rekenen op repercussie door de AP.

4.9 Niet afwachten!

De wetgeving met betrekking tot het melden van datalekken is een feit en wordt nog eens bekrachtigd door de introductie van de AVG. We weten wel dat deze zaken, details daargelaten, allang geregeld en gemeengoed hadden moeten zijn. Maar de praktijk met de waan van alledag vormt doorgaans een stevige hindernis. Er zullen op nationaal niveau en wellicht ook op Europese schaal nog nadere aanwijzingen van toezichthouders en wellicht jurisprudentie moeten volgen over de verwachtingen bij en de uitleg van de interpretabele punten in de wetgeving. Echter, de kat uit de boom kijken en nog even helemaal niet in actie komen tot het zover is betekent een grote kans op achterstand en daardoor, in geval van pech, verwijtbare nalatigheid en dus mogelijk een forse boete. Nú investeren in de meldplicht datalekken betaalt zich straks bovendien nogmaals uit wanneer het boeteregime van de veel strengere AVG in werking treedt. Een groot deel van de bepalingen van de meldplicht komt in de AVG immers terug.

Maar bedenk vooral dit: het is allemaal te doen geweest om de klant/burger een betere positie te geven om zijn privacy te kunnen verdedigen. Dat maakt een goed georganiseerde en transparante privacybescherming tot een kwaliteitsaspect van de dienstverlening. En bij uitstek past het de overheidsorganisaties om daarin het voortouw te nemen en het voorbeeld te stellen. De burger is allang de controle over zijn privacy kwijt. Wat nog rest is de morele plicht om zorgvuldig met zijn gegevens om te gaan. Ook private organisaties kunnen zich hiermee positief onderscheiden. *Business as usual*, toch*?*

[32] We doelen hier op de beoogde betere bescherming en rechtspositie van betrokkenen.

[33] Zie: Elisabeth Thole e.a.: De algemene meldplicht datalekken en de cyberverzekering. in: Tijdschrift aansprakelijkheids- en verzekeringsrecht in de praktijk #2, SDU, November 2015.

Colofon

Dit CIP-document is een product van de Domeingroep Privacy, een van de vijf thematische domeingroepen in CIP-verband. Teksten en (links naar) aanvullende documentatie zijn aangedragen door de domeingroepleden en ook de opeenvolgende kritische reviews zijn 'in eigen huis' gedaan. Uitgave geschiedt onder auspiciën van de Domeingroep Privacy en onder verlening van de Creative Commons licentie zoals op het titelblad staat vermeld.

De oorspronkelijke publicatie van dit stuk (september 2014) is een initiatief van Aramis Jean Pierre (DUO), Gineke Kuipers (DUO) en Ruud de Bruijn (CIP/UWV) naar aanleiding van interne notities van Mieke Anema (UWV) en Hatice Dogan (SVB) na het verschijnen van de eerste versie van het wetsvoorstel "Meldplicht datalekken" in 2013. Diverse leden van de CIP-domeingroep Privacy hebben in reviews en materiaalsuggesties waardevolle bijdragen geleverd. De eindredactie van de updates is in handen van Gineke Kuipers en Ruud de Bruijn.

Amsterdam/Groningen, april-november 2016

Bijlage 1: het wetsvoorstel Gegevensverwerking en meldplicht cybersecurity

Deze "Wet houdende regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)" is op 27 oktober 2016 door de Tweede Kamer als hamerstuk afgedaan[34].

Dit wetsvoorstel sluit aan bij de ambitie van de Europese Commissie om EU-breed te komen tot een meldplicht voor overheden en vitale marktpartijen die bijdraagt aan het verhogen van de digitale veiligheid, zie pag. 33 over de NIB : de ontwerprichtlijn voor netwerk- en informatiebeveiliging.
Hoewel het mogelijk is dat persoonsgegevens geraakt zijn door een inbreuk, of anderszins worden verwerkt bij de uitvoering van de wet, betreft het niet op de eerste plaats privacywetgeving. De minister kan eenieder verzoeken om gegevens te verstrekken ten behoeve van in de wet genoemde doeleinden en taken. In lijn met de Wbp, art 43, wordt expliciet gesteld dat de eis van verenigbaarheid met het doel waarvoor de gegevens oorspronkelijk waren verstrekt (Wbp, art. 9) niet van toepassing is bij een dergelijk verzoek.

Het wetsvoorstel introduceert een meldplicht - onverwijld - voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken. Het doel is om het risico van maatschappelijke ontwrichting als gevolg van ICT-inbreuken in te schatten en die ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken. Deze meldplicht geldt voor aanbieders van producten of diensten waarvan de beschikbaarheid of *betrouwbaarheid van vitaal belang* zijn voor de Nederlandse samenleving ("vitale aanbieders"). Het fundament van en voor het wetvoorstel is de ministeriële verantwoordelijkheid om vitale aanbieders bij te staan "bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van hun producten of diensten te waarborgen of te herstellen" (artikel 2).

Om de drempel laag te houden kent de voorgestelde meldplicht geen sanctiemogelijkheid, wordt het NCSC niet belast met toezicht en handhaving en is de meldplicht primair gericht op het bieden van hulp. Hulp door het NCSC aan de getroffen organisatie behelst het bieden van handelingsperspectief door het geven van advies en informatie en het coördineren van de inzet van andere (overheids)organisaties of daar waar noodzakelijk het bieden van technische ondersteuning om de gevolgen van een inbreuk te beperken.

Het is van belang dat de meldingen in vertrouwen gedaan kunnen worden om kwetsbaarheid te beperken dan wel in de toekomst te vermijden. Het voorstel bevat een aantal bepalingen ter bescherming van de vertrouwelijkheid enerzijds en het verwerken van persoonsgegevens door het NCSC anderzijds.

De vitale aanbieders en hun concrete producten en diensten waarvoor de meldplicht gaat gelden, zullen worden aangewezen bij Algemene maatregel van bestuur (AMvB). De aanwijzing zal in ieder geval zien op partijen uit de sectoren: elektriciteit, gas, drinkwater, telecom, financiën, overheid (waaronder in ieder geval keren en beheren oppervlaktewater) en transport (mainports Rotterdam en Schiphol). Te denken valt daarbij aan vitale aanbieders zoals energienetwerkbeheerders, drinkwaterbedrijven, telecombedrijven, beheerders van hoofdwaterkeringen of banken.

[34] Kamerstuk34388; Voorstel van wet; Memorie van toelichting

De aan te wijzen organisaties in de vitale sectoren zijn niet verplicht om élke ICT-inbreuk aan het NCSC te melden. De verplichting is er alleen als "de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van het aangewezen product of de aangewezen dienst in belangrijke mate wordt of kan worden onderbroken".

Twee problemen, althans: valkuilen schuilen wat ons betreft in deze tekst. Het eerste betreft DDoSaanvallen (Distributed Denial of Service), deze hoeven niet gemeld te worden. De redenering is dat bij een DDoS-aanval weliswaar de bereikbaarheid van een online-dienst wordt aangetast, maar geen aantasting plaatsvindt van de systemen van de online-dienst zelf. Bovendien is de wetgever van mening dat het bij deze aanvallen veelal zal gaan om een tijdelijke beperking van de bereikbaarheid, waardoor "de maatschappelijk ontwrichtende werking […] in het algemeen veel beperkter [is] dan in geval van daadwerkelijke ICT-inbreuken".

Als tweede punt komt daarbij de term 'in belangrijke mate'. Het voornemen is dit in overleg met de betrokken sectoren en departementen nader uit te werken en "daarbij zal mede bepalend zijn onder welke omstandigheden sprake is of kan zijn van 'maatschappelijke ontwrichting'" - wat ook weer zo'n term is…. Partijen hebben natuurlijk wel altijd de mogelijkheid om ernstige verstoringen van de bereikbaarheid vrijwillig aan het NCSC te melden.

Voor enkele sectoren geldt voor ICT-inbreuken al een verplichting tot melding aan de sectorale toezichthouder. De nu voorgestelde meldplicht "sluit aan bij en treedt niet in de thans geldende sectorale bevoegdheden". Daarmee laat de voorgestelde meldplicht ook de bestaande crisisbeheersingsstructuren ongemoeid. De Mvt besteedt uitgebreid aandacht aan overlap en de mogelijkheid dat men verplicht is dubbel (in theorie soms zelfs driedubbel: sectorautoriteit, AP en V&J/NCSC) te melden als er bij incidenten ook persoonsgegevens in het spel zijn.

> *Het advies van de Raad van State en de eerste reacties van de vaste Kamercommissie vertonen nog heel wat vraagtekens[35]. De RvS vraagt zich - met sommige fracties - af of het wetsvoorstel zonder handhaving/sanctionering wel zin heeft, om dezelfde reden als door de regering wordt aangevoerd voor niet-sanctionering: dat de betrokken partijen zelf al hoogst gemotiveerd zullen zijn om inbreuken te voorkomen dan wel zo snel mogelijk te herstellen. Andere vragen vanuit de commissie betreffen de onduidelijkheid in dit stadium over de sectoren/organisaties die de wet zou raken (de nog op te stellen AMvB), het feit dat het NCSC niet bevoegd is tot dadergericht onderzoek, dat er teveel meldplichten (zijn) ontstaan, de onduidelijkheid over lastenverzwaring en men wil graag de PIA zien die voor het wetsvoorstel is uitgevoerd.*

Voor enkele grote publieke uitvoeringsorganisaties in het CIP-netwerk, zoals met name DUO, SVB en UWV, zou dit wel eens een relevante ontwikkeling kunnen zijn. In een lijvig themanummer 'Herijking vitale infrastructuur' van het *Magazine Nationale Veiligheid en Crisisbeheersing* (juli 2015) komen we een overzicht tegen van impactcategorieën waarmee een organisatie kan inschatten of toekomstige wet directe gevolgen zal hebben voor de bedrijfsvoering. Dit overzicht is weergegeven in figuur 5 op de volgende pagina.

[35] Kamerstukken 34388

Onder categorie B, de laatste bullit staat een impactbeschrijving die zo maar van toepassing zou kunnen zijn wanneer de dienstverlening van genoemde organisaties (voor langere tijd) geblokkeerd zou zijn.

CATEGORIE A
In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de vier impactcriteria voor categorie A raakt:
- economische gevolgen: meer dan ca. 50 miljard euro schade of ca. 5.0 % daling reëel inkomen;
- fysieke gevolgen: meer dan 10.000 personen dood, ernstig gewond of chronisch ziek;
- sociaal maatschappelijke gevolgen: meer dan 1 miljoen personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen;
- cascadegevolgen: uitval heeft als gevolg dat minimaal twee andere sectoren uitvallen.

CATEGORIE B
In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria voor categorie B raakt:
- economische gevolgen: meer dan ca. 5 miljard euro schade of ca. 1.0 % daling reëel inkomen;
- fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek;
- sociaal maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen.

Fig. 5

Magazine nationale veiligheid en crisisbeheersing 2015 - nr. 3 | 5

Over hoe en bij welke instantie(s) de meldingen moeten worden gedaan worden nog nadere regels gesteld. Vooralsnog zijn dit de contouren:
- De meldplicht geldt alleen voor bij AMvB aan te wijzen aanbieders van daarbij aan te wijzen producten of diensten; de meldplicht zal ook gelden voor de financiële sector en de overheid zelf.
- De melding moet worden gedaan aan de Minister van Veiligheid en Justitie en wordt behandeld door het Nationaal Cyber Security Centrum (NCSC);
- Het NCSC kan vervolgens:
  - inschatten hoe groot de impact is;
  - hulp verlenen aan de getroffen aanbieder;
  - andere vitale aanbieders waarschuwen.

Bij een melding worden in ieder geval de volgende elementen verwacht:
- De aard en omvang van de inbreuk of het verlies;
- Zo mogelijk het tijdstip van de aanvang van de inbreuk of het verlies;
- De mogelijke gevolgen van de inbreuk of het verlies;
- Een prognose van de hersteltijd;
- Zo mogelijk de door de vitale aanbieder genomen of te nemen maatregelen om de gevolgen van de inbreuk of het verlies te beperken of herhaling hiervan te voorkomen;
- De contactgegevens van de in Nederland gevestigde functionaris die verantwoordelijk is voor het doen van de kennisgeving.

Desgevraagd levert de melder tevens:
- de informatie die nodig is voor een inschatting van de risico's voor de beschikbaarheid of betrouwbaarheid van de producten of diensten, alsook:
- alle informatie die nodig is om de melder bij te staan de beschikbaarheid of de betrouwbaarheid te waarborgen of te herstellen.

Het wetsvoorstel bevat voorts nog enkele bepalingen omtrent het vertrouwelijk omgaan met en eventueel doorgeven van de verstrekte gegevens door de minister.

De relevante passages in de Mvt over de mogelijke samenloop van meldplichten vind je in Bijlage 3Bijlage 3Bijlage 3Bijlage 3. Heel overzichtelijk vinden wij het niet. De volgende 'vuistregels' helpen wellicht:

1. Bestaande sectorale meldplichten voor incidenten blijven zoals ze zijn; het is nog onduidelijk hoe de meldplicht bij NCSC voor ICT-inbreuken zich hiertoe gaat verhouden.

2. Meldplichten in diezelfde sectoren waarbij persoonsgegevens betrokken zijn en die voldoen aan de kenmerken zoals gesteld in de meldplicht datalekken moeten worden gemeld bij de Autoriteit Persoonsgegevens.
   Indien het tevens incidenten betreft die al meldplichtig waren, betekent dat dus dubbel melden: bij de AP en bij de sectorale autoriteit. Is het tevens een ICT-inbreuk dan zou daar zelfs een melding aan NCSC bij kunnen komen.

3. De bestaande sectorale meldplicht aan de ACM voor incidenten met persoonsgegevens uit hoofde van de Telecommunicatiewet komt te vervallen. Daarvoor in de plaats komt regel 2.

4. Melding aan betrokkenen conform de meldplicht datalekken is altijd aan de orde indien het risico op ernstige nadelige gevolgen aanwezig wordt geacht, *behalve* wanneer het incident zich afspeelt binnen de financiële sector.

Bijlage 2: De AVG en het Europese perspectief

Er is, in ieder geval op Europese schaal, een tendens naar (zoveel mogelijk uniforme) privacy wet- en regelgeving die verbetering beoogt van de bescherming en de positie van burgers/klanten/betrokkenen. Materieel moeten zij vooral gedragsverandering bij gegevensverwerkende organisaties bewerkstelligen: openheid en eerlijkheid. Deze organisaties, overheid en commercie, krijgen dit nu te verwerken en dat kost moeite. Maar zij moeten gaan beseffen dat een verbeterd vertrouwen van consumenten op termijn profijtelijk zal zijn voor de zaak die zij voorstaan.

De AVG

De AVG heet in de Nederlandstalige versie *Verordening (EU) 2016/679 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). Deze verordening vloeit voort uit artikel 4 lid 5 van de herziene Richtlijn 2002/58/EG*[36]. De Verordening is een vervolg op de Privacy Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

> *Naast de Algemene verordening gegevensbescherming is er ook een Richtlijn gegevensbescherming in het kader van de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten. Beide documenten moeten met elkaar in samenhang worden gezien en vormen samen het nieuwe rechtskader voor de bescherming van persoonsgegevens binnen de Europese Unie (EU).*
> *In tegenstelling tot een richtlijn, hoeft een verordening niet te worden geïmplementeerd in nationale wetgeving: zij is rechtstreeks in alle lidstaten van kracht. Dit neemt niet weg dat de verordening zoals nu aangenomen nog op veel plaatsen nationale invulling vergt - of daar in ieder geval nadrukkelijk de ruimte voor open laat.*
> *De NL versie is, naast de EN-versie en andere vertalingen, via deze link te downloaden; klik HIER om direct naar de NL-versie te gaan*[37]*. Let wel: de EN-versie is leidend.*

De Algemene Verordening Gegevensbescherming (GDRP: General Data Protection Regulation) is op 25 mei 2016 aangenomen in het Europese parlement. De wetteksten van de Verordening en de Richtlijn zijn op 4 mei 2016 in het Publicatieblad van de Europese Unie gepubliceerd[38]. Op 6 mei 2018 moeten de EU-lidstaten de Richtlijn hebben omgezet in nationale wetgeving. Vanaf 25 mei 2018 is de Verordening van toepassing. Verantwoordelijken voor verwerkingen van persoonsgegevens, bewerkers, providers, toezichthouders, de nationale wetgever etc. hebben dus gedurende 2 jaar de gelegenheid om de nodige maatregelen te treffen teneinde aan de eisen van de Verordening te voldoen. Gedurende de invoeringsperiode kunnen burgers al wel een beroep doen op de bepalingen van deze nieuwe wetgeving, maar handhaving kan pas na deze periode starten.
De eerste officiële 'draft' van de tekst is uitgebracht op 25 januari 2012. De AVG 'final' heeft er dus ruim 4 jaar over gedaan en is in die tijd, met name nog in de laatste paar maanden, flink aangepast.

[36] Bij het opstellen van de deze Uitvoeringsverordening is ook rekening gehouden met het advies van de Groep Gegevens-bescherming Artikel 29 over het ontwerpbesluit van de Commissie betreffende maatregelen voor het melden van inbreuk en in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie d.d. 12 juli 2012 (WP197).
[37] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679; http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN.
[38] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf; https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijn_2016_-_680_definitief.pdf

De AVG in het algemeen en daarmee ook de bepalingen omtrent 'Personal data breach' gaan over bescherming van burgers en in zoverre is er grote gelijkenis met de motieven voor de Nederlandse datalekwetgeving. De burger krijgt de beschikking over meer expliciete mogelijkheden tot verbetering van zijn positie ten opzichte van organisaties die beschikken over gegevens over hem. Deze organisaties moeten doordrongen worden van het recht op privacy en het recht op controle daarop door de betrokkene. Dit geldt voor alle verantwoordelijken en hun bewerkers, maar het zijn vooral de grote wereldspelers geweest die met datavergaring en -verkoop als verdienmodel de aanleiding hebben gegeven tot de astronomische boetebedragen en de 'accountability' en aansprakelijkheid die nu in de AVG staan. Grote monopolisten, overheidsorganisaties daarbij inbegrepen, plegen zich eigener beweging niet altijd veel aan te trekken van privacyrechten. De AVG gaat daarom over verandering van gedrag, en daarvoor overtuigen redelijke argumenten alléén kennelijk onvoldoende.

De in de Wbp geregelde meldplicht datalekken komt ook in de AVG voor. Er is echter een belangrijk verschil in het criterium op grond waarvan een datalek gemeld moet worden: op grond van de Wbp moeten alleen 'ernstige' lekken gemeld worden. Op grond van de AVG moeten alle lekken aan de toezichthouder gemeld worden, tenzij de verwerkingsverantwoordelijke conform het verantwoordings-beginsel kan aantonen dat het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich brengt. De verwerker onder de AVG (in de Wbp bewerker) krijgt een eigen, zelfstandige verplichting om de verwerkingsverantwoordelijke zonder onredelijke vertraging van een inbreuk op de hoogte te stellen. Verwerkers hebben momenteel alleen de meldplichten die hen contractueel worden opgelegd door hun klanten (verwerkingsverantwoordelijke). Dat verandert onder het regime van de AVG. Partijen moeten overigens nog steeds afspraken maken over de wijze waarop de verwerker bijstand zal verlenen in het geval van een inbreuk (artikel 28 lid 3)[39].

We kunnen in het bestek van deze notitie niet op de AVG-details ingaan. Voor nu willen we vooral benadrukken dat 'onze' meldplicht datalekken voor een flink deel vooruitloopt op de AVG variant 'Personal data breach' en dat het dus alleszins de moeite waard is om daarmee vast aan de slag te gaan. Dat zal geen verloren moeite zijn en zeker zijn vruchten afwerpen in de implementatieperiode van de AVG. Want de verordening is, vergeleken met de meldplicht, strenger: bestuurlijke verantwoordelijkheid en aansprakelijkheid, een concreet compliancy-voorschrift en hogere boetes[40]. Met de meldplicht data-lekken en de daarvoor benodigde incidentadministratie kun je de organisatie al heel behoorlijk daarop voorbereiden. Plus dat de AVG nog wat (verwante) zaken met zich meebrengt, wier realisatie eveneens veel aandacht en tijd zal gaan vergen, zoals bijvoorbeeld 'the right to be forgotten', waarop klanten/burgers zich in bepaalde gevallen kunnen gaan beroepen, en de mogelijkheid om gevrijwaard te blijven van beslissingen die op basis van geautomatiseerde besluitvorming (lees ook: profiling) tot stand komen. Google heeft er inmiddels al een flinke kluif aan.

Nationale invulling

Een zeer opmerkelijk kenmerk van de eindversie ten opzichte van de eerdere AVG-concepten vinden wij het grote aantal plaatsen dat nog nadere nationale invulling of interpretatie behoeft. Dat maakt het voorlopig ook wel weer lastig om op alle onderdelen trefzeker te kunnen anticiperen op de feitelijke invoering in 2018. Hoewel er op veel van die punten allang nationale wetgeving bestaat (in Nederland in of via de WBP, maar ook de wet- en regelgeving voor politie-, inlichtingen- en veiligheidsdiensten en dergelijke), is het toch steeds de vraag welke keuzes de politiek voor de BV Nederland zal maken. Zo is het hierboven genoemde vergeetrecht in de eindversie toch weer aan de nationale invulling overgelaten, en

[39] Passage uit *Algemene Verordening Gegevensbescherming* van SVB, 30 september 2016, interne memo geschreven door Hatice Dogan (FG van SVB); (publicatie is gevraagd en toegestaan).

[40] Art. 83: tot €20 mln. of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is. Dit is overigens substantieel lager dan wat in de laatste concepten stond: resp. €100 mln. of 5%.

geldt de verplichte aanstelling van een Functionaris voor de Gegevensbescherming in organisaties met 250+ Fte's in de eindversie (artikel 37 AVG) nog slechts voor *overheids*organisaties[41], waarbij overigens geen sprake meer is van een minimum aantal Fte's[42].
Voor overheidsinstanties is ook deze interessant: of zij net als iedere andere organisatie boetes opgelegd kunnen krijgen voor overtredingen van de AVG wordt aan de nationale wetgever overgelaten.

Deze en andere punten zijn verzameld in een interessant en misschien ook wel onthutsend overzicht, zie het artikel "Brengt de privacyverordening werkelijk uniform Europees privacyrecht?" van Mark Jansen op 21 april 2016 op de site van *Dirkzwager/Intellectuele eigendom en IT*.

De WBP
Het is de verwachting dat deze 'AVG-exegese' in een nationale uitvoeringswet terecht zal komen, een 'lidstatelijke' voetnoot bij de AVG met restanten uit de WBP - en/of nieuwe voorschriften. Maar tot het zover is blijft de WBP en verwante wetgeving natuurlijk gewoon van kracht en kun je je daarop richten. Een tip voor niet-juristen: in de CIP publicatie "Privacy Baseline" vind je snel en concreet wat er in de organisatie geregeld moet zijn volgens de WBP[43].

Overige privacywetgeving
Op meer plaatsen is of wordt gewerkt aan de (wettelijke) bescherming van de privacy van burgers, waarbij ideeën worden uitgewerkt die overeenkomen met die welke aan de AVG ten grondslag liggen. Er is sowieso oog voor het Europese perspectief bij het ontwikkelen van privacywetgeving.
Het Nederlandse Wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens in de zorg bijvoorbeeld, ingediend in december 2012 reeds, maar aangehouden door de Eerste Kamer, bevat o.a. ook aanpassingen van de WBP en behandelt 'het recht op informatie', toestemming tot elektronische inzage en het recht om de toestemming in te trekken, en de relatie tussen patiënt en behandelaar waarbij de behandelaar gegevenstechnisch als een bewerker van gegevens wordt gezien. Zie onder andere de "*Samenvatting wetsvoorstel cliëntenrechten bij elektronische gegevensverwerking*" in de uitgave Wet- en regelgeving in de zorg van Nictiz. Ook een verplichte aanstelling van een Functionaris voor de gegevensbescherming behoort nu tot de plannen[44].

In dit rijtje past ook de al eerder genoemde en in 2012 aangenomen Gewijzigde Telecommunicatiewet, met eveneens verbetering van de positie van telecomconsumenten, doordat aanbieders betere informatie moeten verschaffen over af te sluiten abonnementen, en met een meldplicht bij inbreuken op de beveiliging waarbij persoonsgegevens zijn gelekt.

---

[41] Dat is niet helemaal waar: lid 1 van art. 37 AVG duidt ook op verwerkers van gegevens uit grootschalige/langdurige/stelselmatige/gevoelige observatie. Zoals wij dat lezen kunnen dat ook niet-overheden zijn:
De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan in elk geval waarin: a) de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken; b) een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of c) de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.

[42] In aanvulling: artikel 37 zegt ook dat de FG moet worden aangesteld "indien dat Unierechtelijk of lidstaatrechtelijk is verplicht". Dat zou kunnen gaan gelden voor zorginstellingen (zie de paragraaf over het Elektronisch Patiëntendossier op pagina 32).

[43] "Grip op Privacy: de Privacy Baseline. De Wbp ontrafeld voor toepassing in organisaties, v1.0. CIP publicatie november 2015.

[44] Zover nu bekend wordt het wetsvoorstel eind september (2016) behandeld; voor de status en voortgang zie: https://www.eerstekamer.nl/wetsvoorstel/33509_clientenrechten_bij

Verwant op Europees niveau is ook de ontwerprichtlijn over netwerk- en informatiebeveiliging (NIB). Het doel van het NIB-voorstel is een veilige en betrouwbare digitale omgeving in de gehele EU tot stand te brengen. Burgers en consumenten moeten meer vertrouwen krijgen in de technologieën, diensten en systemen die zij dagelijks gebruiken. Ook hier geldt een meldplicht, en de gelijkenis met het Nederlandse wetsvoorstel Gegevensverwerking en meldplicht cybersecurity zal wel niet toevallig zijn. Op 5 juli 2016 hield het Europees Parlement een debat over dit voorstel en 6 juli 2016 stemde het ermee in, zie hiervoor:

http://www.europa-nu.nl/id/vjv757lq1wx4/nieuws/netwerk_en_informatiebeveiliging?ctx=vj6ykc608htw&tab=0.
http://www.europa-nu.nl/id/vk5jhn9b9tz5/nieuws/cybersecurity_ep_steunt_regels_om_vitale?ctx=vj6ykc608htw&tab=0
https://www.eerstekamer.nl/eu/edossier/e130011_voorstel_voor_een
http://www.consilium.europa.eu/nl/press/press-releases/2015/06/29-network-information-security/

Ten slotte: in verband met de verschuiving naar Europese wetgeving is het nuttig om ENISA, het *European Network and Information Security Agency* in de gaten te houden. Ook de AVG verwijst ernaar.

Bijlage 3: Over sectorale toezichthouders en dubbele meldingen

Integraal overgenomen uit: Memorie van toelichting bij de meldplicht datalekken (finale versie)

Verhouding tot andere rechtsgebieden

4.1 Verhouding tot specifieke meldplicht op grond van de Telecommunicatiewet

Een sterk vergelijkbare meldplicht voor inbreuken op de beveiliging van persoonsgegevens is reeds opgenomen in artikel 11.3a van de Telecommunicatiewet (Tw). Dit artikel vormt de implementatie van de in artikel 2, onderdeel 4, van richtlijn 2009/136/EG[1] opgenomen regeling die aanbieders van openbare elektronische communicatiediensten verplicht tot het melden van doorbrekingen van de maatregelen die zijn getroffen om persoonsgegevens te beveiligen. Vanwege de reikwijdte van deze richtlijn geldt de meldplicht op grond van artikel 11.3a van de Tw uitsluitend voor aanbieders van openbare elektronische communicatiediensten. Naar aanleiding van het grote aantal gevallen waarin bij andere bedrijven dan de aanbieders van openbare elektronische communicatiediensten sprake was van tekortkomingen in de beveiliging van persoonsgegevens, wordt deze meldplicht met dit wetsvoorstel aangevuld met een meldplicht voor alle verantwoordelijken voor de verwerking van persoonsgegevens, zowel in de private als publieke sector.

Eén toezichthouder voor meldplicht datalekken Wbp/Tw

Aanbieders van openbare elektronische communicatiediensten moeten momenteel op grond van artikel 11.3a van de Tw de melding bij de Autoriteit Consument en Markt (ACM) (voorheen: OPTA) doen. Om redenen van doelmatigheid worden beide meldplichten zoveel als mogelijk is onderling op elkaar afgestemd. Om die redenen wordt ook voorgesteld de melding op grond van artikel 11.3a van de Tw bij het Cbp te beleggen. Hierbij moet worden bedacht dat de beveiligingsplicht die op de aanbieders van openbare elektronische communicatienetwerken en -diensten rust krachtens artikel 11.3 van de Tw zonodig reeds door het Cbp kan worden gehandhaafd. Immers, de bevoegdheid van het Cbp om toezicht op de naleving uit te oefenen strekt zich volgens artikel 51, tweede lid, van de Wbp tot alle vormen van verwerking van persoonsgegevens, waarbij alleen de reikwijdtebepalingen van de Wbp grenzen stellen aan de bevoegdheid. Dit doet er niet aan af dat ACM primair belast blijft met het toezicht op de naleving van artikel 11.3 van de Tw. In lijn met het overgaan van de toezichtstaken van ACM naar Cbp worden de nodige toezichts- en sanctiebevoegdheden op artikel 11.3a Tw (geregeld in hoofdstuk 15 van de Tw) aan het Cbp verleend. Dat is geregeld in artikel II, onderdelen C tot en met F. De bestuurlijke boete die het Cbp bij overtreding van de artikelen 34a van de Wbp en artikel 11.3a van de Tw zal kunnen opleggen bedraagt €450.000. Voor het overige verandert er niets in de verhouding tussen Wbp en Tw. De OPTA gaat er in haar advies dan ook terecht van uit dat dit wetsvoorstel ook geen verandering brengt in de uitleg van artikel 11.3a van de Tw, zoals die is gegeven in de memorie van toelichting die leidde tot dat wetsvoorstel. De OPTA merkt in haar advies ook terecht op dat artikel 11.3a van de Tw alleen een meldplicht oplegt die verband houdt met de levering van openbare elektronische communicatiediensten. Wanneer zich een datalek zou voordoen bij, bijvoorbeeld, de personeelsadministratie van een aanbieder van deze diensten, dan zal gemeld moeten worden overeenkomstig de Wbp, en niet de Tw. Voor de praktische uitvoering van de meldplicht van de Wbp zal zoveel mogelijk worden aangesloten bij de voorschriften die de Europese Commissie binnenkort zal vaststellen met tot de meldplicht van artikel 11.3a van de Telecommunicatiewet (uitvoeringsverordening van de Europese Commissie op grond van richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (COCOM12–25REV2).

---

[1] Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (PbEU L 337). Artikel 2, onderdeel 4, van richtlijn 2009/136/EG bevat een wijziging van artikel 4, derde lid, van richtlijn 2002/58/EG die tot doel heeft een bestaande zeer beperkte meldplicht voor bijzondere risico's voor de gevolgen van inbreuken op de beveiliging van elektronische communicatienetwerken en -diensten voor de persoonlijke levenssfeer uit te breiden.

Samenwerking Cbp-ACM
De voorgestelde voorziening heeft consequenties voor de samenwerking tussen Cbp en ACM. De reeds bestaande samenwerking zal geïntensiveerd worden. Er bestaat reeds een samenwerkingsprotocol tussen beide bestuursorganen. Mogelijk moet dit protocol worden herzien. Wellicht willen Cbp en ACM voor wederzijdse informatievoorziening ook enkele organisatorische voorzieningen treffen. Dat blijft aan de ACM en het Cbp om te bepalen. Wel is in artikel I, onderdeel C, van het wetsvoorstel, mede naar aanleiding van het advies van het Cbp, voorzien in een wettelijke grondslag voor deze samenwerkingsrelaties. Voor de ACM bestaat die grondslag al in artikel 18.3 van de Tw.

4.2 Verhouding tot meldplicht incidenten Wet op het financieel toezicht
De voorgestelde meldplicht voor datalekken zal ook van toepassing zijn op de financiële sector, zij het in beperkte vorm. Een financiële onderneming wordt namelijk niet verplicht om datalekken te melden aan betrokkenen. Dit is in lijn met de reeds lang onder de Wet op het financieel (hierna: Wft) bestaande praktijk dat een financiële onderneming incidenten wel moet melden aan de financieel toezichthouder, maar niet aan betrokkene. De overweging is dan ook dezelfde: dergelijke openbare kennisgevingen aan betrokkenen zijn in de financiële sector – mede tegen de achtergrond van de financiële crisis – te risicovol om dwingend te worden voorgeschreven. Onvoorspelbaar is of een openbare kennisgeving kan leiden tot het ontstaan van geruchten die niet meer op zakelijke wijze ontzenuwd kunnen worden en die daardoor nodeloos aanleiding geven tot vermindering van vertrouwen van het publiek of de relevante markt. De zorgplicht van de financiële onderneming zal echter waarborgen dat zij ook zonder dat dit dwingend wordt voorgeschreven haar verantwoordelijkheid jegens haar cliënten in rechtstreeks contact met die cliënten zal nemen. Dit doet zij nu al met betrekking tot incidenten onder de Wft en dat zal niet anders zijn ten aanzien van datalekken onder dit wetsvoorstel. Aanvankelijk was in de geconsulteerde versie van het wetsvoorstel een uitzondering op de meldplicht opgenomen voor de financiële sector. Naar aanleiding van de consultatiereactie van De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) is het tiende lid gewijzigd. De uitzondering van financiële ondernemingen als bedoeld in de Wet op het financieel toezicht (Wft) is ingeperkt. De reden voor deze wijziging van het tiende lid is dat de uitzondering van de financiële sector in de consultatie-versie te ruim was. In die versie hoefde een financiële onderneming die een incident als bedoeld in de Wft2 moet melden aan de financieel toezichthouder, geen datalek te melden aan het Cbp en betrokkene. Deze uitzondering is te ruim omdat een incident als bedoeld in de Wft niet altijd een datalek is (een ernstig gevaar voor de integere bedrijfsuitoefening wordt niet altijd veroorzaakt door een datalek); het omgekeerde geldt ook: een datalek is niet altijd een incident (niet alle datalekken vormen een ernstig gevaar voor de integere bedrijfsuitoefening). Door de te ruime uitzondering zouden derhalve de datalekken die niet tevens incident zijn buiten beeld blijven van een toezichthouder. In het kader van de administratieve lasten voor financiële ondernemingen wordt nog kort iets opgemerkt over eventuele dubbele meldplichten voor de financiële sector. *Deze dubbele meldplicht zal alleen bestaan als een datalek eveneens een incident is; alsdan moet zowel aan het Cbp als aan DNB of de AFM worden gemeld*. [cursief door redactie] Informatie verkregen van de financiële sector leert echter dat er in de afgelopen twee jaar een tiental incidenten is gemeld. Als we zouden aannemen dat al deze incidenten tevens datalekken zijn, gaat het dus slechts om een vijftal dubbele meldingen per jaar. Daarbij kan nog worden opgemerkt dat deze dubbele meldingen te rechtvaardigen zijn vanuit de verschillende doelen van de betreffende meldplichten. Het doel van de plicht om datalekken te melden aan het Cbp is om een grotere transparantie bij de verwerking van persoonsgegevens te bewerkstelligen, om ruimere aandacht te genereren voor de noodzaak om goed te investeren in beveiligingsmaatregelen en om op den duur toename van het vertrouwen van de samenleving in de geautomatiseerde verwerking van persoonsgegevens te bewerkstelligen. Het doel van de plicht om incidenten te melden aan DNB of de AFM is om de integere uitoefening van het bedrijf van de desbetreffende financiële onderneming te bewaken, waarborgen of herstellen. Het is derhalve belangrijk dat de financiële toezichthouders in kennis worden gesteld van alle incidenten en het Cbp van alle onder de meldplicht vallende datalekken, ook al leidt dat in een enkel geval tot een dubbele meldplicht voor financiële ondernemingen.

Bronnenoverzicht
Gebruikte of genoemde informatiebronnen en aanvullend materiaal.

De meldplicht datalekken
"Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp)":
https://www.rijksoverheid.nl/documenten/publicaties/2015/07/10/staatsblad-230-wijziging-van-de-wet-bescherming-persoonsgegevens
https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2015/07/10/staatsblad-230-wijziging-van-de-wet-bescherming-persoonsgegevens/wet-meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-stb-2015-2-2.pdf
https://www.rijksoverheid.nl/documenten/publicaties/2015/07/10/staatsblad-230-wijziging-van-de-wet-bescherming-persoonsgegevens
https://www.rijksoverheid.nl/actueel/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-1-januari-2016-van-kracht

De Memorie van toelichting:
https://www.eerstekamer.nl/behandeling/20130617/memorie_van_toelichting_4/document3/f=/vjc76lpx9ryk.pdf

De meldplicht datalekken, overzicht vanaf 2013:
https://www.eerstekamer.nl/wetsvoorstel/33662_meldplicht_datalekken_en

Over de meldplicht datalekken
Op de site van de Autoriteit Persoonsgegevens (https://autoriteitpersoonsgegevens.nl) is zeer veel informatie en toelichting te vinden, onder andere:

De Beleidsregels:
"De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). Beleidsregels voor toepassing van artikel 34a van de Wbp". Autoriteit Persoonsgegevens, 8 dec 2015.
https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-beleidsregels-meldplicht-datalekken;
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken.pdf.

"De Boetebeleidsregels Autoriteit Persoonsgegevens 2016" (Staatcourant Nr.2043, 15 januari 2016):
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebeleidsregels_autoriteit_persoonsgegevens_staatscourant_2016-2043_0.pdf

Over het melden:
https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken#publications

Een zeer complete behandeling van de aspecten van de meldplicht die van belang zijn voor organisaties biedt onder andere:
Hutter, J. e.a., "*Grip op datalekken*", december 2015, Wolters Kluwer:
http://www.wolterskluwer.nl/shop/grip-op-datalekken/prodNPGRIDATA.html?gclid=CK2PkdzwsMwCFRBmGwodP9ICKg
NB: Let er wel op dat de auteurs in deze publicatie nog moesten verwijzen naar de consultatieversie van de Beleidsregels en dat de latere definitieve publicatie van 8 december daarvan afwijkt.

Een goede en (medio 2016) actuele compacte samenvatting is hier te vinden:
https://ictprivacyrecht.nl/files/2015/10/Factsheet-impact-van-de-meldplicht-datalekken.pdf
Zie daar ook van Peter Kager (30 december 2015):
https://ictprivacyrecht.nl/datalekken/vijf-misverstanden-over-de-meldplicht-datalekken

Overige gemelde of gebruikte bronnen in verband met de meldplicht
IBD: Factsheet Meldplicht datalekken. Goede 2-pager over de meldplicht en de voorbereiding daarop.
https://www.ibdgemeenten.nl/wp-content/uploads/2015/03/15-0312-Factsheet_Meldplicht-Datalekken_LR-DEF-1.pdf

Anton Ekker - "*In 4 stappen voldoen aan de meldplicht datalekken*". NICTIZ, Whitepaper sept. 2012:
https://www.nictiz.nl/publicaties/in-vier-stappen-voldoen-aan-de-meldplicht-datalekken1

Huub de Jong "*Klaar voor een datalek*", Madison Gurkha, januari 2016
https://www.madison-gurkha.com/press/MeldplichtDatalekken.pdf
https://www.nictiz.nl/SiteCollectionDocuments/Whitepapers/Whitepaper%20meldplicht%20datalekken%20versie%201.0.pdf

Privacy Barometer (27 mei 2015):
https://www.privacybarometer.nl/maatregel/41/Meldplicht_datalekken_en_uitbreiding_boetebevoegdheid

Fig. over de voorbereiding op de nieuwe wetgeving is afkomstig uit:
https://www.sebyde.nl/wet-meldplicht-datalekken

Op de site van de Informatie Beveiligingsdienst (IBD, www.ibdgemeenten.nl) staat, naast nuttige tips en verwijzingen, een mooie model-bewerkersovereenkomst:
https://www.ibdgemeenten.nl/wp-content/uploads/2016/04/16-0426-Bewerkersovereenkomst-v1.2.pdf

Over kosten en risico:
Ponemon Institute (2016): "This year's study found the average consolidated total cost of a data breach grew from $3.8 million to $4 million. The study also reports that the average cost incurred for each lost or stolen record containing sensitive and confidential information increased from $154 to $158. In addition to cost data, the global study puts the likelihood of a material data breach involving 10,000 lost or stolen records in the next 24 months at 26 percent."
http://www-03.ibm.com/security/data-breach/
https://securityintelligence.com/cost-of-a-data-breach-2016/

http://www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-First-Half-2015-Breach-Level-Index.aspx: over de eerste helft van 2015: Wereldwijd 888 (bekende) datalekken plaats, 246 miljoen records (+10% t.o.v. 2014); 53 procent van alle datalekken en 75 procent van de aangetaste bestanden word gebruikt voor identiteitsdiefstal.
Zie ook: http://breachlevelindex.com/#sthash.GkyTie4y.dpbs

Elisabeth Thole e.a.: De algemene meldplicht datalekken en de cyberverzekering. in: Tijdschrift aansprakelijkheids- en verzekeringsrecht in de praktijk #2, SDU, November 2015.
https://www.vandoorne.com/globalassets/publicaties/2015/q4/tav-meldplicht-datalekken-en-cyber-verzekering-november-2015.pdf

Advocaat Aldo Verbruggen in artikelen van Rob de Lange in het Financieel Dagblad, 24 oktober 2016 "Melden van cybercrime zou bijdragen aan het algemeen belang. Ik betwijfel dat zeer" en "Niet melden cybercrime is vaak verstandiger".

Boetes: http://www.wetboek-online.nl/wet/Sr/23.html
Exhibitieplicht: http://www.wetboek-online.nl/wet/BW3/15i.html
WOB: https://www.rijksoverheid.nl/onderwerpen/kwaliteit-en-integriteit-overheidsinstanties/vraag-en-antwoord/wat-is-de-wet-openbaarheid-van-bestuur-wob
Archiefwet: https://www.nationaalarchief.nl/wetten-regelgeving/archiefwet

Gewijzigde Telecommunicatiewet (2012):
https://www.rijksoverheid.nl/actueel/nieuws/2012/06/04/gewijzigde-telecommunicatiewet-in-werking-op-5-juni.

Overige wetten en voorstellen

Wet gegevensverwerking en meldplicht cybersecurity
"Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)"
Kamerstukken 34388:
https://zoek.officielebekendmakingen.nl/behandelddossier/34388
Voorstel van wet:
https://www.eerstekamer.nl/wetsvoorstel/34388_wet_gegevensverwerking_en
https://zoek.officielebekendmakingen.nl/behandelddossier/34388/kst-34388-2?resultIndex=5&sorttype=1&sortorder=4
Memorie van toelichting:
https://zoek.officielebekendmakingen.nl/behandelddossier/34388/kst-34388-3?resultIndex=3&sorttype=1&sortorder=4
https://www.eerstekamer.nl/behandeling/20130617/memorie_van_toelichting_4/document3/f=/vjc76lpx9ryk.pdf
Tweede Kamer, nader rapport inzake wet gegevensverwerking en meldplicht cybersecurity:
https://www.rijksoverheid.nl/regering/inhoud/bewindspersonen/klaas-dijkhoff/documenten/kamerstukken/2016/01/21/tk-nader-rapport-inzake-wet-gegevensverwerking-en-meldplicht-cybersecurity

Over de vitale infrastructuur:
Themanummer "*Herijking vitale infrastructuur*" van het Magazine Nationale Veiligheid en Crisisbeheersing (juli 2015):
https://www.nctv.nl/actueel/nieuws/2015/HerijkingvitaleinfrastructuurcentraalinnieuwsteMagazineNationaleVeiligheidenCrisisbeheersing.aspx
https://www.nctv.nl/binaries/magazine-nationale-veiligheid-en-crisisbeheersing-2015-3_tcm31-29649.pdf

Nationaal Cyber Security Centrum (NCSC): https://www.ncsc.nl

AVG (GDPR)
"Verordening (EU) 2016/679 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming *(Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation))"*
Nederlands: http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679
Engels: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
NB: de Engelse tekst is leidend.
de Verordening niet verwarren met de (verwante en tegelijk aangenomen): "Richtlijn (EU) 2016/680 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad *(Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA)"*
Nederlands: http://eur-lex.europa.eu/legal-content/EN-NL/TXT/?uri=CELEX:32016L0680&from=NL
Engels: http://eur-lex.europa.eu/legal-content/EN-NL/TXT/?uri=CELEX:32016L0680&from=EN
Zie Bijlage 2 over het verschil tussen de Verordening en de Richtlijn.

DSB-MIT-SYSTEM® "*The EU general data protection regulation (GDPR) is published and will take effect in May 25 2018. Regrettably Brussels does not deliver a good readable text for 99 articles and 173 recitals. We fill in this blank.*"
http://www.privacy-regulation.eu/nl/

De teksten van de verordening en de richtlijn zijn ook te vinden bij de Autoriteit Persoonsgegevens:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijn_2016_-_680_definitief.pdf

Over de AVG
De 'oude' privacyrichtlijn:
Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Een aardig overzichtsartikel (gedateerd, maar de geboden inhoud heeft er niet veel last van) is van de hand van:
Jan-Jan Lowijs, 19 februari 2016 "*Een eerste indruk van de Algemene Verordening Gegevensbescherming (AVG)*"
http://blog.euroforum.nl/veiligheid/een-eerste-indruk-van-de-algemene-verordening-gegevensbescherming-avg-2/

Algemene Verordening Gegevensbescherming van SVB, 30 september 2016, interne memo geschreven door Hatice Dogan (FG van SVB); (publicatie is gevraagd en toegestaan).

Mark Jansen, diverse artikelen op de site van Dirkzwager/Intellectuele eigendom en IT:
21 april 2016 "*Brengt de privacyverordening werkelijk uniform Europees privacyrecht?*":
http://dirkzwagerieit.nl/2016/04/21/brengt-de-privacyverordening-werkelijk-uniform-europees-privacyrecht/
25 mei 2016: "*Privacyverordening over twee jaar van toepassing; is uw organisatie daar straks op tijd klaar voor?*"
http:// http://dirkzwagerieit.nl/2016/05/25/privacyverordening-over-twee-jaar-van-toepassing-is-uw-organisatie-daar-straks-op-tijd-klaar-voor/

6 juni 2016 "*Valkuil onder komend privacyrecht*":
http://dirkzwagerieit.nl/2016/06/15/valkuil-onder-komend-privacyrecht-avg-voortaan-alle-beveiligingsinbreuken-loggen-niet-alleen-de-meldingsplichtige/
15 juli 2016: "*Het nieuwe regime voor bijzondere persoonsgegevens onder de privacyverordening: wetgever aan zet om bestaande situatie te behouden*"
http://dirkzwagerieit.nl/2016/07/15/het-nieuwe-regime-voor-bijzondere-persoonsgegevens-onder-de-privacyverordening-wetgever-aan-zet-om-bestaande-situatie-te-behouden/

Overige gemelde of gebruikte bronnen
Ontwikkelingen in Europese wetgeving:
Ontwerprichtlijn over netwerk- en informatiebeveiliging (NIB):
http://www.europa-nu.nl/id/vjv757lq1wx4/nieuws/netwerk_en_informatiebeveiliging?ctx=vj6ykc608htw&tab=0
http://www.europa-nu.nl/id/vk5jhn9b9tz5/nieuws/cybersecurity_ep_steunt_regels_om_vitale?ctx=vj6ykc608htw&tab=0
Voorstel voor een richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen:
https://www.eerstekamer.nl/eu/edossier/e130011_voorstel_voor_een
Persbericht over de NIB (29 juni 2015):
http://www.consilium.europa.eu/nl/press/press-releases/2015/06/29-network-information-security/

European Union Agency for Network and Information Security (ENISA):
https://www.enisa.europa.eu
https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
Procure Secure: A guide to monitoring of security service levels in cloud contracts (ENISA)
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport

Over cliëntenrechten
"Wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens in de zorg" (2012)
https://www.eerstekamer.nl/wetsvoorstel/33509_clientenrechten_bij
"*Samenvatting wetsvoorstel cliëntenrechten bij elektronische gegevensverwerking*" in de uitgave Wet- en regelgeving in de zorg van Nictiz (pagina 8 e.v.)
https://www.nictiz.nl/SiteCollectionDocuments/Boeken/Wet-%20en%20regelgeving%20in%20de%20zorg.pdf

Van Oortmarssen, Koers en De Bruijn "*Grip op Privacy: de Privacy Baseline. De Wbp ontrafeld voor toepassing in organisaties, v1.0*" CIP publicatie november 2015.
https://www.cip-overheid.nl/wp-content/uploads/2015/11/20151130_Privacy_Baseline_v1_0.pdf

Organisatie en rollen:
Roles and Responsibilities. The short answer is everyone is responsible for IT security awareness and training. Some organizations have a mature IT security program, while other organizations may be struggling to achieve this goal because of staffing, funding, and management support. Security awareness and training programs therefore vary greatly from one organization to the next. One way to help ensure that a program matures is to develop and document IT security awareness and training responsibilities for those key positions upon which the success of the program depends.
http://www.trustnetinc.com/Training/security-awareness-responsibilities.html

"Privacy Governance onderzoek: Volwassenheid van privacybeheersing binnen Nederlandse organisaties",
PwC Nederland, Februari 2015. https://www.pwc.nl/nl/assets/documents/pwc-privacy-governance-onderzoek.pdf

Juridisch Kompas (20131111_Juridisch_Kompas_versie_2_0.pdf) Interne UWV studie/notitie. Relevantie met name: Norm 5: Borging uitvoering privacyrechten klant en Norm 6: Borging goede bewijspositie [verkrijgbaar via de redactie].

Marcel Koers "*Grip op beveiligingsovereenkomsten*" CIP oktober 2014. Over een andere manier van omgang tussen opdrachtgever en leverancier, teneinde een zo goed mogelijke samenwerking en een optimaal resultaat te bewerkstelligen. Relevantie: regel hierin ook rollen en aansprakelijkheden ivm privacy-schadeclaims.
http://www.cip-overheid.nl/wp-content/uploads/2014/10/Grip-op-Beveiligingsovereenkomsten-v1_0.pdf

Kenmerken van een cyberaanval
Gaat het netwerk plat? Verslag van de tweede bijeenkomst van de mastercourse 'Cybersecurity voor management en bestuur'. Gemeentehuis Weert, woensdag 7 augustus 2012, directieteamvergadering, 11.30 uur. De deur gaat open, iemand van de ICT-afdeling. "Er is een virus actief in het netwerk. Er zijn twee besluiten nodig. Gaat het netwerk plat? En gaan we ermee naar buiten?" http://ibestuur.nl/academie/gaat-het-netwerk-plat