Wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de verruiming van de mogelijkheid van het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving en de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (gebruik camerabeelden en meldplicht datalekken) *(versie consultatie en advies - dec 11)*

MEMORIE VAN TOELICHTING

Algemeen

1. Doel van het wetsvoorstel

In dit wetsvoorstel wordt een verruiming voorgesteld van de mogelijkheid om door particulieren vervaardigde camerabeelden van strafbare feiten te benutten voor de ondersteuning van de rechtshandhaving. Verder wordt in dit wetsvoorstel een meldplicht geïntroduceerd voor verantwoordelijken voor de verwerking van persoonsgegevens in geval van gebleken doorbrekingen van de getroffen maatregelen ter beveiliging van persoonsgegevens. Het nalaten aan deze verplichting te voldoen wordt gesanctioneerd met een bestuurlijke boete.

2. Beleidsmatige achtergrond

In paragraaf 10 "Veiligheid" van het regeerakkoord "Vrijheid en verantwoordelijkheid" van 30 september 2010 zet het kabinet krachtig in op meer cameratoezicht. In dezelfde paragraaf kondigt het kabinet een voorstel aan voor een meldplicht voor alle aanbieders van diensten van de informatiemaatschappij, waaronder de overheid, in geval van verlies, diefstal of misbruik van persoonsgegevens (hierna ook: datalekken). Daarbij moeten alle datalekken worden gemeld aan de nationale toezichthouder die boetes kan opleggen indien de meldplicht niet wordt nageleefd. Beide maatregelen zijn nauw met elkaar verbonden. Cameratoezicht bevordert het zichtbaar maken van criminaliteit en overlast in de fysieke wereld, waardoor een meer effectieve bestrijding van deze verschijnselen mogelijk wordt. De meldplicht datalekken bevordert het zichtbaar worden van de consequenties voor burgers van computercriminaliteit of vormen van verwijtbare nalatigheid bij de beveiliging van gegevens in de digitale wereld. Transparantie bevordert dat overheden, bedrijven en burgers zorgvuldiger met persoonsgegevens omgaan en hun verplichting die gegevens te beveiligen tegen verlies of onrechtmatige verwerking serieuzer nemen.

Bij brief van 29 april 2011 van eerste en tweede ondergetekende aan de voorzitters van de Eerste en de Tweede Kamer der Staten-Generaal (Kamerstukken II 2010/11, 32 761, nr. 1) en de daarbij behorende Notitie privacybeleid is een aantal wetgevingsvoornemens geformuleerd die moeten worden uitgevoerd. Aan deze maatregelen hechten wij onverminderd groot belang. Echter, een aantal omstandigheden maken nadere keuzes met betrekking tot het moment waarop en het tempo waarin deze maatregelen worden uitgevoerd onvermijdelijk. Beide ondergetekenden hebben dit in een algemeen overleg met de Vaste Commissie voor Veiligheid en Justitie uit de Tweede Kamer der Staten-Generaal op 15 september 2011 toegelicht. In de brief van de Staatssecretaris van Veiligheid en Justitie van 27 oktober 2011 aan de voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 2011/12, 32 761, nr. 4) is dit nog eens bevestigd.

In de zomer van 2011 is - andermaal - duidelijk geworden dat de criminaliteit in de vorm van overvallen op en diefstal uit winkels of inbraken die gepaard gaan met vernielingen, gevolgd door diefstal bij burgers en bedrijven, een diepe indruk maken op slachtoffers van deze misdrijven. Vaak treffen burgers en bedrijven zelf de nodige beveiligingsmaatregelen tegen deze vormen van criminaliteit. De installatie van beveiligingscamera's is een doelmatige beveiligingsmaatregel. Camerabeelden van strafbare feiten blijken een nuttig hulpmiddel bij de opsporing van deze strafbare feiten. Hoe sneller de beelden bij politie en justitie beschikbaar zijn, hoe groter de kans op een succesvolle opsporing van het strafbare feit en het achterhalen van de verdachten is, zo blijkt in de praktijk telkens weer. Ook blijkt dat het tonen van deze beelden aan het publiek een zinvolle ondersteuning van de opsporing kan zijn.
Wanneer echter niet alle mogelijkheden om de beelden optimaal te gebruiken worden benut, dan leidt dat tot gevoelens van frustratie en teleurstelling bij de slachtoffers en mogelijk ook tot het verminderen van het vertrouwen in opsporing en vervolging. Dit kan ertoe leiden dat burgers overgaan tot het zelfstandig plaatsen van camerabeelden op internet zonder betrokkenheid van politie en justitie. De bedoeling daarvan is verklaarbaar. Men wenst reacties van het publiek te verzamelen die kunnen leiden tot de aanhouding van de daders. Echter, de effecten daarvan

kunnen onder omstandigheden negatief zijn. Soms worden personen op ondoordacht verspreide beelden ten onrechte in verband gebracht met strafbare feiten. Er is dan sprake van een schending van de privacy van deze burgers. Ook bestaat het risico dat de opsporingsbelangen worden doorkruist. Het is heel goed denkbaar dat de opsporingsbelangen in een individuele zaak vergen dat geen publiciteit wordt gegeven aan een bepaald strafbaar feit. Opsporingsberichtgeving is niet primair een voorlichtingsmiddel, maar een opsporingsinstrument van politie en justitie.
Waar het ondergetekenden vooral om gaat is dat de privacywetgeving het gebruik van camerabeelden van particulieren als ondersteuning van de opsporing niet meer, maar ook niet minder moet reguleren dan strikt noodzakelijk is om een evenwichtige benadering tussen de bescherming van persoonsgegevens en de belangen van opsporing en vervolging van strafbare feiten te bereiken.
De maatschappelijke discussie die hoog is opgelopen, vergt dat de privacywetgeving op dit onderdeel een bescheiden herijking ondergaat, zodat een wat ruimer gebruik van door particulieren vervaardigde camerabeelden als ondersteuning van de opsporing mogelijk wordt, zonder de belangen van de bescherming van persoonsgegevens te verminderen. Die herijking moet met een zekere urgentie worden doorgevoerd om tegemoet te komen aan de verwachting die de samenleving hiervan heeft. Het is om die reden dat een nader toe te lichten voorziening in de Wbp (artikel I, onderdelen B en C, van dit wetsvoorstel) wordt toegevoegd aan een ander voorstel tot wijziging van de Wbp dat met urgentie moet worden ontwikkeld, de meldplicht datalekken.

Naar aanleiding van een groot aantal incidenten waarbij door een inbreuk op de beveiliging van, onder meer, websites persoonsgegevens vrijkwamen met nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, wordt in dit wetsvoorstel een meldplicht voor dergelijke inbreuken ingevoerd. De verantwoordelijke moet op grond van het voorgestelde artikel 34a van de Wet bescherming persoonsgegevens (Wbp) (artikel I, onderdeel D, van het wetsvoorstel) bij een inbreuk melding doen bij het College bescherming persoonsgegevens (Cbp). Als niet aan deze meldplicht wordt voldaan zal het Cbp bevoegd zijn een bestuurlijke boete op te leggen. Hiermee wordt tevens invulling gegeven aan het regeerakkoord "Vrijheid en verantwoordelijkheid" van 30 september 2010.
De meldplicht die in dit wetsvoorstel is opgenomen heeft uitsluitend betrekking op doorbrekingen van de maatregelen voor de beveiliging van persoonsgegevens. De meldplicht ziet dus niet op situaties als die rond DigiNotar waarin fouten werden gemaakt in de beveiliging van certificaten waardoor deze onbetrouwbaar waren, of op andere meldplichten met een min of meer verwant karakter. Op de verhouding van de meldplichten uit dit wetsvoorstel met evenbedoelde andere meldplichten wordt in paragraaf 4.2 nog teruggekomen.
Dat neemt niet weg dat alle meldplichten met betrekking tot datalekken, of andere ernstige incidenten met betrekking tot de bedrijfsvoering, en in het bijzonder de informatiehuishouding, van bedrijven en overheid - ongeacht welke inhoud zij hebben en ongeacht of zij vrijwillig of verplichtend, of privaatrechtelijk of publiekrechtelijk van aard zijn - wel steeds hetzelfde doel dienen. Dat doel is het bevestigen en waar nodig herstellen van het vertrouwen dat de desbetreffende instelling of bedrijf van het publiek, de klanten, de markt, de overheid en de toezichthouders in de desbetreffende instelling of het desbetreffende bedrijf heeft.
Wat de Wbp betreft, geldt dat de wetgever door middel van algemeen-abstract geformuleerde normen, een relatief grote mate van vrijheid, en dus ook vertrouwen, geeft aan de bedrijven, instellingen en burgers die onder de reikwijdte van de wet vallen. Bij het geven van vertrouwen hoort echter ook het afleggen van een zekere mate van rekenschap aan samenleving en de kringen van betrokkenen. Wanneer er een reëel risico is voor verlies of onrechtmatige verwerking van persoonsgegevens, of wanneer dat risico zich heeft verwezenlijkt, kan dat vertrouwen in meer of minder ernstige mate worden geschaad. Het is in het belang van zowel de verantwoordelijke als de betrokkene dit vertrouwen zo snel mogelijk te herstellen. Transparantie over de aard van het datalek, de vermoedelijke omvang ervan en aard van de mogelijke schade, de inspanningen die gepleegd worden om de schade te herstellen en raadgevingen aan publiek en klanten om zichzelf zo goed mogelijk in staat te stellen de consequenties voor de eigen belangen te overzien zijn noodzakelijke maatregelen voor behoud en herstel van dat vertrouwen. Dat vertrouwen wordt ondersteund doordat onafhankelijke toezichthouders in staat worden gesteld zich een eigen beeld te vormen van de feiten, een oordeel kunnen geven over de genomen maatregelen, onder omstandigheden vertrouwelijk met de verantwoordelijke kunnen overleggen en zonodig kunnen interveniëren. Als sluitstuk op het geheel wordt het nalaten aan deze verplichting te voldoen gesanctioneerd met een bestuurlijke boete.

3. Gebruik van camerabeelden vervaardigd door particulieren

3.1 Algemeen

Cameratoezicht moet, wanneer met behulp van een camera individuele personen herkenbaar in beeld worden gebracht, worden aangemerkt als een vorm van verwerking van persoonsgegevens. De Wbp geeft regels ter bescherming van de persoonlijke levenssfeer en persoonsgegevens. De Wbp kent echter geen specifieke bepalingen over cameratoezicht. Wel bevat artikel 38 van het Vrijstellingsbesluit Wbp voorwaarden waaronder de verantwoordelijke die met behulp van cameratoezicht persoonsgegevens verwerkt met het oog op de beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen is vrijgesteld van de verplichting deze verwerking te melden bij het Cbp.
Uit de artikelen 33 en 34 van de Wbp vloeit voort dat cameratoezicht kenbaar moet worden gemaakt met bord of algemeen begrijpelijk symbool. Heimelijk cameratoezicht is in beginsel alleen toelaatbaar na een voorafgaand onderzoek door het Cbp.
Wanneer de opnamen beelden bevatten van te identificeren personen die buiten redelijke twijfel strafbare feiten begaan, dan moet de verwerking van deze beelden worden aangemerkt als de verwerking van strafrechtelijke persoonsgegevens. Daarmee vallen deze beelden binnen de reikwijdte van het verbod, neergelegd in artikel 16 van de Wbp, om bijzondere persoonsgegevens te verwerken.
Op dat verbod zijn een ruim aantal uitzonderingen geformuleerd. Artikel 22, eerste lid, van de Wbp zondert de gegevensverwerking door de politie en het openbaar ministerie uit, voor zover deze plaatsvindt krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens. Gegevensverwerking krachtens de artikelen 2 en 6 van de Politiewet 1993 valt ook overigens in algemene zin buiten de reikwijdte van de Wbp. De Wbp staat daarom niet in de weg aan het gebruik van camerabeelden afkomstig van particulieren door politie en openbaar ministerie bij de uitoefening van hun taken.
In de Aanwijzing Opsporingsberichtgeving van het College van procureurs-generaal van 16 februari 2009 (Stcrt. 51) zijn richtlijnen gegeven voor de gevallen waarin openbaar ministerie en politie deze beelden gebruiken, en op internet en andere manieren onder de aandacht van het publiek brengen.
Een andere uitzondering op het verbod is dat de verantwoordelijke op grond van artikel 22, tweede lid, onder b, van de Wbp strafrechtelijke gegevens mag verwerken ter bescherming van zijn belangen voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn. Een verantwoordelijke heeft op grond van deze uitzondering de mogelijkheid camerabeelden waarop te identificeren personen zichtbaar zijn te verwerken ten behoeve van de bescherming van zijn eigen belangen, en die van het personeel dat in zijn dienst is. Als voorbeeld voor deze toepassing kan worden gedacht aan camerabewaking in een winkel. De winkelier heeft dan de mogelijkheid beelden te maken en te bewaren met het oog op voorkoming en bestrijding van winkeldiefstal door klanten of fraude door het personeel. Gebruik van de beelden is dan in elk geval mogelijk bij het doen van aangifte van diefstal, of als bewijsvoering in een ontslagzaak.
Het is niet zonder meer mogelijk de aldus verwerkte beelden ook ten behoeve van derden te verwerken. Artikel 22, vierde lid, van de Wbp geeft daarvoor drie mogelijkheden.
Allereerst is het mogelijk door middel van de diensten van een particulier beveiligingsbedrijf of recherchebureau camerabeelden te laten vervaardigen. Het betrokken bedrijf moet dan wel beschikken over een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus. Deze eis heeft de wetgever gesteld, omdat met het vergunningvereiste is verzekerd dat het betrokken bedrijf voldoet aan de eisen van professionaliteit. Bovendien voorziet de wet in overheidstoezicht op de beveiligingsbranche.
Een andere mogelijkheid is dat de verantwoordelijke die deel uitmaakt van een groep in vennootschapsrechtelijke zin de beelden kan delen met andere rechtspersonen die deel uitmaken van die groep. Dat brengt met zich dat de beelden zonodig kunnen worden gedeeld in concernverband. Het nuttig effect hiervan kan aanzienlijk zijn. Zo is het denkbaar dat beelden van een overval, een inbraak of een diefstal kunnen worden gedeeld met alle filialen van een bepaalde onderneming.
Tenslotte kan verwerking van de beelden plaatsvinden wanneer passende en specifieke waarborgen zijn getroffen en de verantwoordelijke voor de verwerking de procedure van een voorafgaand onderzoek in de zin van artikel 31 van de Wbp heeft gevolgd. Wanneer deze procedure wordt gevolgd, meldt de verantwoordelijke de verwerking bij het Cbp aan. Het Cbp beoordeelt vervolgens of het aanleiding ziet een nader onderzoek te verrichten. Dit onderzoek mondt uit in een besluit van het Cbp omtrent de rechtmatigheid van de verwerking. Dit onderzoek duurt geruime tijd.
In de hiervoor genoemde brief van de Staatssecretaris van Veiligheid en Justitie aan de voorzitter van de Tweede Kamer der Staten-Generaal van 27 oktober 2011 is de conclusie getrokken dat de uitzondering op het verbod om strafrechtelijke gegevens te verwerken door politie en justitie afdoende is geregeld. Ten aanzien van de andere twee uitzonderingen, het gebruik door particuliere beveiligingsorganisaties en overig gebruik, is anders geoordeeld.

Zoals in paragraaf 2 van deze memorie al is aangegeven, is het gebruik van beelden een nuttig middel bij opsporing en vervolging. Bovendien is het beeldmateriaal in ruime mate beschikbaar en ontbreekt het burgers en bedrijven niet aan de bereidheid het beschikbaar te stellen. Een meer efficiënte benutting van het beeldmateriaal verhoogt daarom de kansen op een meer succesvolle opsporing. Daar komt bij dat de overheid burgers ook aanspreekt op hun vermogen zelf te investeren in hun eigen veiligheid. Als zij dit doen en de resultaten van hun investeringen vervolgens niet of nauwelijks bijdragen aan een veiliger samenleving, dan zal de bereidheid tot investeren niet toenemen.
Aan een meer efficiënte benutting van het beeldmateriaal kan op twee manieren worden bijgedragen. Ten eerste is het denkbaar dat beelden die worden verwerkt door particuliere beveiligingsorganisaties ook buiten de relatie tussen beveiligingsbedrijf en opdrachtgever kunnen worden verwerkt. Dat zal moeten gebeuren onder voorwaarden die in het belang van de opsporing en vervolging van strafbare feiten en het belang van de bescherming van persoonsgegevens moeten worden gesteld. Ten tweede is het denkbaar dat particulieren zelf in staat worden gesteld de beelden te verspreiden, eveneens wanneer wordt voldaan aan voorwaarden die het primaat van de overheid bij de opsporing en vervolging van strafbare feiten veiligstellen en voorwaarden in het belang van de bescherming van persoonsgegevens.
Concreet kan aan de volgende toepassingen worden gedacht. Winkelcentra en winkels worden in zeer veel gevallen beveiligd met behulp van cameratoezicht. Soms is sprake van een eenvoudig, door een winkelier zelf opgezet systeem. Grote winkelpanden en winkelcentra zijn dikwijls uitgerust met professionelere systemen die worden bediend door personeel in dienst van beveiligingsbedrijven.
In de winkelcentra en in grotere afzonderlijke winkels zijn daarnaast vaak beeldschermen aangebracht. Met die beeldschermen wordt doorgaans de aandacht van het publiek gezocht voor hetgeen in de winkel of het winkelcentrum wordt aangeboden. Die beeldschermen zijn in beginsel ook geschikt om de opgenomen beelden van strafbare feiten te tonen aan het bezoekend publiek. Langs die weg kan een potentieel groot aantal mogelijke getuigen worden bereikt. Het tonen van de beelden zou dan gecombineerd moeten worden met een verzoek om melding te maken van relevante feiten bij de beveiligingsorganisatie of aangifte te doen bij de politie. Een dergelijke mogelijkheid behoort alleen te worden geboden wanneer het openbaar ministerie daarvoor toestemming verleent. De eerdergenoemde Aanwijzing opsporingsberichtgeving voorziet in algemene zin al in een afwegingskader voor het gebruik van de diverse vormen van opsporingsberichtgeving. Daarbij moeten steeds afwegingen van proportionaliteit, subsidiariteit en de relatieve zwaarte van de inbreuk op de privacy worden betrokken. De Aanwijzing voorziet bovendien in een regeling die verwijdering van de beelden mogelijk maakt, wanneer bijvoorbeeld blijkt dat sprake is van het door een verdachte of veroordeelde bewust gebruikmaken van de identiteit van een ander, waardoor ten onrechte sprake kan zijn van het openbaarmaken van persoonsgegevens. Deze voorwaarden behoren voor de in dit wetsvoorstel voorgestelde voorziening niet anders te zijn.
Overigens sluit deze voorziening aan bij reeds door de Aanwijzing opsporingsberichtgeving bestreken gevallen waarin met behulp van billboards in de openbare ruimte of in het openbaar vervoer beelden kunnen getoond. Gebruik van dit middel na de ongeregeldheden bij het Feyenoordstadion in Rotterdam in september 2011 leidde tot de aanhouding van vele verdachten.
Naast deze mogelijkheid is het zeker denkbaar dat onder omstandigheden ook aan particulieren een wat ruimere mogelijkheid kan worden geboden tot verwerking van camerabeelden, buiten de hierbovengenoemde gevallen waarin dit toegestaan, zonder dat de omslachtige en langdurige procedure van het voorafgaand onderzoek dor het Cbp moet worden gevolgd. Omdat de ervaring leert dat het tonen van camerabeelden aan het publiek alleen zinvol kan worden ingezet wanneer dit kort na de opgenomen gebeurtenissen plaatsvindt, heeft het volgen van die procedure van het voorafgaand onderzoek meestal niet veel zin.
Ook voor deze mogelijkheid geldt dat het primaat van de opsporing van strafbare feiten een overheidszaak blijft. Dat betekent dat ook voor deze mogelijkheid geldt dat hoe dan ook eerst aangifte wordt gedaan van een strafbaar feit en dat politie en justitie eerst de gelegenheid moeten hebben de beelden te beoordelen op bruikbaarheid voor de opsporing. Politie en openbaar ministerie moeten eerst zelf de mogelijkheid krijgen de beelden via de eigen middelen te gebruiken. Het zal daarom ook onvermijdelijk zijn dat toestemming van het openbaar ministerie nodig is, voordat tot verdere verspreiding via private middelen wordt overgegaan. Het geven van toestemming zal alleen onder voorwaarden mogelijk zijn. Een aantal daarvan zijn hierboven al genoemd, zoals het voorafgaand doen van aangifte. Andere voorwaarden kunnen betrekking hebben op de wijze van openbaarmaking, de duur van de openbaarmaking en de zorg voor de doelmatige verwijdering van de beelden.
Bij de kring van personen voor wie deze regeling mogelijk van belang kan zijn, hoeft niet noodzakelijkerwijs alleen aan individuele burgers gedacht te worden. Het kan ook van belang zijn voor openbaarvervoerbedrijven, decentrale overheden, of voor het publiek toegankelijke

instellingen als openbare bibliotheken. Ook die bedrijven en instellingen beschikken immers over verschillende andere mogelijkheden tot openbaarmaking, zoals billboards.
De voorwaarden waaronder de beelden door particuliere beveiligingsdiensten en door andere particulieren kunnen worden verwerkt zullen bij algemene maatregel van bestuur verder worden uitgewerkt. Het gaat bij die uitwerking om normen met een min of meer gedetailleerd niveau. De Wbp bevat vooral algemeen geformuleerde normen van een hoog abstractieniveau. Bovendien past een delegatieconstructie ook systematisch in het geheel van artikel 22 van de Wbp. Het zevende lid van die bepaling bevat immers reeds een delegatiegrondslag.
Met dit wetsvoorstel wordt uitvoering gegeven aan de door de Tweede Kamer aanvaarde motie van de leden Elissen en Van Toorenburg (Kamerstukken II 2011/12, 33 000 VI, nr. 53). Zolang burgers en bedrijven zich bij het zelf op internet plaatsen van beelden bewegen binnen de voorwaarden die op grond van dit wetsvoorstel worden gesteld - en die bij algemene maatregel van bestuur nader worden ingevuld - is die vorm van gegevensverwerking rechtmatig en hoeft er dus niet te worden gevreesd voor enige vorm van sanctionering. Worden die grenzen overschreden, dan ligt dit natuurlijk anders.

3.2 Toetsing aan richtlijn 95/46/EG

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 (PbEG L 281) (hierna: de richtlijn) bevat geen specifieke bepalingen met betrekking tot de verwerking van persoonsgegevens in de vorm van camerabeelden van personen in het algemeen, of van personen betrokken bij strafbare feiten in het bijzonder. Met betrekking tot de verwerking van strafrechtelijke gegevens is de hoofdregel van artikel 8, vijfde lid, van de richtlijn dat deze gegevens alleen mogen worden verricht onder toezicht van de overheid, of indien de nationale wetgeving voorziet in passende specifieke waarborgen. In afwijking daarvan kunnen de lidstaten nationale bepalingen vaststellen welke passende en specifieke waarborgen bevatten. Artikel 8, vijfde lid, van de richtlijn bevat daarom een voldoende ruime grondslag voor een verfijning van de tekst van artikel 22 van de Wbp om de in paragraaf 3.1 van deze memorie voorgestelde maatregel mogelijk te maken.
In artikel 20, eerste lid, van de richtlijn wordt aan de lidstaten overgelaten aan te geven welke verwerkingen mogelijk specifieke risico's voor de persoonlijke rechten en vrijheden inhouden, zodanig dat zij voor de aanvang van de verwerking moeten worden onderzocht. Die bepaling is geïmplementeerd in artikel 31 van de Wbp. Artikel 20 van de richtlijn geeft de lidstaten een zekere beleidsmarge bij de invulling van deze bepaling. De specifieke risico's voor de persoonlijke rechten en vrijheden bij de verwerking van strafrechtelijke gegevens in de vorm van camerabeelden buiten de thans bestaande mogelijkheden op grond van artikel 22, vierde lid, van de Wbp kunnen beter worden gedekt met algemeen verbindende voorschriften dan met het blijven stellen van de eis dat in elk individueel geval een voorafgaand onderzoek moet plaatsvinden. Het positieve effect dat de beschikbaarstelling en verdere verspreiding van camerabeelden heeft, wordt tenietgedaan als deze betrekkelijk omslachtige procedure steeds wordt gevolgd. Dit rechtvaardigt de voorgestelde wijziging van artikel 31 van de Wbp in voldoende mate.

4. Meldplicht datalekken

Met een zekere regelmaat verschijnen in de media berichten over de blootstelling van persoonsgegevens aan de openbaarheid, doordat de verantwoordelijke onvoldoende beveiligingsmaatregelen heeft genomen om de persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking, of door een inbreuk op deze beveiligingsmaatregelen. In een aantal gevallen betrof het zeer ernstige schendingen, waarbij de ernst zowel betrekking had op het aantal persoonsgegevens als op de aard van de gegevens. Het is mede daarom dat in het regeerakkoord "Vrijheid en verantwoordelijkheid" van 30 september 2010 is overeengekomen dat alle diensten van de informatiemaatschappij, ook als die door de overheid worden aangeboden, zullen worden onderworpen aan een meldplicht voor inbreuken op de beveiliging waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking van persoonsgegevens, waaraan nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkene zijn verbonden. In artikel I, onderdeel D, van dit wetsvoorstel (het voorgestelde artikel 34a van de Wbp) wordt daaraan uitvoering gegeven. In het regeerakkoord wordt daar nog aan toegevoegd dat de naleving van deze meldplicht gesanctioneerd wordt met een bestuurlijke boetebevoegdheid voor het Cbp. Daaraan wordt uitvoering gegeven in artikelen I, onderdeel E, en II, onderdeel E, van het wetsvoorstel.
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 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 elektronische communicatiediensten. Naar aanleiding van het grote aantal gevallen waarin bij andere bedrijven dan de aanbieders van 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.
Aanbieders van elektronische communicatiediensten moeten momenteel op grond van artikel 11.3a van de Tw de melding bij het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (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 OPTA primair belast blijft met het toezicht op de naleving van artikel 11.3 van de Tw.
Indien in een inbreukgeval zowel artikel 11.3a van de Tw als artikel 34a van de Wbp in beginsel van toepassing zijn, en de verantwoordelijke dezelfde persoon is als de aanbieder van de elektronische communicatiedienst, hoeft deze uitsluitend op grond van artikel 11.3a van de Tw een melding te doen. In dat geval hoeft hij in zijn hoedanigheid als verantwoordelijke geen melding meer te doen op grond van artikel 34a van de Wbp. Artikel 34a, negende lid, van de Wbp bevat daarvoor een voorziening. Is de verantwoordelijke die op grond van artikel 34a van de Wbp meldingsplichtig is, een ander dan de aanbieder van de elektronische communicatiedienst die op grond van artikel 11.3a van de Tw meldingsplichtig is, bijvoorbeeld omdat die aanbieder de bewerker in de zin van de Wbp is, dan moeten beide partijen voldoen aan hun meldplicht.
In lijn met het overgaan van de toezichts- en handhavingstaken van OPTA naar Cbp worden ook de nodige opsporings- en sanctiebevoegdheden voor het toezicht 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 € 200.000,=.

4.1 Nieuwe voorziening in de Wet bescherming persoonsgegevens

4.1.1 Verhouding Wet bescherming persoonsgegevens en Telecommunicatiewet

Bij de vormgeving van de nieuwe voorziening in de Wbp is, met het oog op de doelmatigheid van het toezicht, zoveel mogelijk aangesloten bij artikel 11.3a van de Tw. Artikel 11.3a van de Tw blijft dus van toepassing op aanbieders van elektronische communicatiediensten. Wel wordt voorgesteld dat ook deze melding voortaan bij het Cbp moet worden gedaan, in plaats van bij OPTA, zodat het Cbp toezicht houdt op de naleving van beide meldplichten bij inbreuken op de beveiliging van persoonsgegevens.
Niettemin blijven er enige noodzakelijke verschillen in formulering bestaan tussen het voorgestelde artikel 34a van de Wbp en artikel 11.3a van de Tw. Artikel 11.3a van de Tw is de implementatie van artikel 4, derde lid, van richtlijn 2002/58/EG. Om niet af te wijken van deze bepaling is ervoor gekozen artikel 11.3a van de Tw te behouden voor de gevallen waarop het nieuwe artikel 4, derde lid, van richtlijn 2002/58/EG ziet. Die omstandigheid maakt dat in artikel 11.3a van de Tw zo nauw mogelijk moet worden aangesloten bij de formulering van die richtlijn. Overwogen is om artikel 34a van de Wbp op dezelfde wijze te formuleren. Hiervan is om twee redenen afgezien.

[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.

Allereerst geldt dat de voorziening in de Wbp uit oogpunt van uitvoerbaarheid bij voorkeur zoveel mogelijk zou moeten aansluiten bij de beveiligingsplicht van artikel 13 van de Wbp. Die bepaling bevat immers een omschrijving van de risico's die de beveiligingsplicht moet afdekken. Die omschrijving is zelf weer terug te voeren op artikel 17 van richtlijn 95/46/EG en daarmee ook niet geheel vrijblijvend.
Belangrijker is dat artikel 4, derde lid, van richtlijn 2002/58/EG geen enkele clausulering of beperking bevat van de aard van de gevallen die gemeld moeten worden. Zou die keuze worden overgenomen in de Wbp, dan zou dat kunnen leiden tot een overvloed aan meldingen die de meldplicht mogelijk kan uithollen, en bovendien aanleiding geeft tot onnodig hoge bestuurlijke en administratieve lasten. De reikwijdte van de Wbp is immers veel groter dan die van de Tw. Die negatieve effecten moeten zoveel mogelijk worden voorkomen. Om die reden is een voorziening voor het voorkomen van nodeloze meldingen in het wetsvoorstel opgenomen, die in paragraaf 4.1.4 wordt toegelicht. Hoewel die voorziening is opgenomen is het voorgestelde artikel 34a, eerste lid, van de Wbp, waar een meldplicht van de verantwooordelijke aan het Cbp is geregeld, heeft die voorziening ook consequenties voor de meldplicht van de verantwoordelijke aan de betrokkene. Artikel 11.3a, tweede lid, van de Tw bevat bij die meldplicht de voorwaarde "indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer". Die voorwaarde hoeft niet te worden herhaald in het voorgestelde artikel 34a, tweede lid, van de Wbp. Uit artikel 34a, eerste lid, van de Wbp volgt voldoende duidelijk onder welke beperkende omstandigheden er een meldplicht bestaat. Door de in artikel 34a, tweede lid, van de Wbp opgenomen verwijzing naar het eerste lid is voldoende duidelijk dat de beperkende omstandigheden uit het eerste lid ook gelden voor de meldplicht uit het tweede lid. Er is daarom geen materieel verschil tussen de artikelen 34a, tweede lid, van de Wbp en 11.3a, tweede lid, van de Tw.

4.1.2 Verantwoordelijke en bewerker

Het voorgestelde artikel 34a van de Wbp richt zich tot de verantwoordelijke. De verantwoordelijk is immers krachtens artikel 13 van de Wbp gehouden de nodige beveiligingsmaatregelen te treffen. Ook overigens vloeit uit de systematiek van de Wbp dat verplichtingen zijn gericht tot de verantwoordelijke, en niet tot anderen. De verantwoordelijke behoort zich, in het belang van de bescherming van de door hem verwerkte gegevens, aan de betrokkene bekend te maken, zodat deze zonodig zijn rechten kan uitoefenen. Dat geldt ook in de gevallen waarin een verantwoordelijke zich bedient van een bewerker. Weliswaar zal de bewerker de partij zijn die feitelijk belast is met het ten uitvoer leggen van de passende technische en organisatorische maatregelen in de zin van artikel 13 van de Wbp ter beveiliging van de verwerkte gegevens, maar artikel 14, derde lid, onder b, van de Wbp legt de verantwoordelijke expliciet een zorgplicht op voor het nakomen van deze verplichting. Daaraan kan hij zich niet onttrekken. Artikel 14, vijfde lid, van de Wbp verplicht bovendien tot een schriftelijke (of daarmee als gelijkwaardig aan te merken) vastlegging van, onder meer, de beveiligingsmaatregelen waarop artikel 13 van de Wbp het oog heeft. Deze regels zijn gesteld in het belang van de betrokkene en de verantwoordelijke. Zodoende is de verhouding tussen verantwoordelijke en bewerker door de wetgever in belangrijke mate ingekleurd door hetgeen de beveiligingsplicht met zich brengt. Dit is zodanig zwaarwegend dat de regeling van de meldplicht ook moet doorwerken in deze rechtsverhouding. Het is bovendien van belang met het oog op de werking van de specifieke aansprakelijkheids- en schadevergoedingsregeling van artkel 49 van de Wbp. Die regeling richt zich primair tot de verantwoordelijke en niet tot de bewerker. Om een meer evenwichtige regeling te bereiken, wordt voorgesteld dat de zorgplichten van de verantwoordelijke op grond van artikel 14 van de Wbp zich expliciet uitstrekken over datalekken waarvan de bewerker kennis krijgt, onverminderd de eindverantwoordelijkheid van de verantwoordelijke (artikel I, onderdeel A, van het wetsvoorstel). Dit alles betekent dat de meldplicht zich uitstrekt tot iedere verantwoordelijke in de zin de van de Wbp. Het is niet relevant of de verantwoordelijke een natuurlijke persoon of rechtspersoon is. Evenmin is relevant of de verantwoordelijke deel uitmaakt van de publieke of de private sector. Wel is het zo dat de kring van verantwoordelijken voor wie de meldplicht geldt wordt beperkt door de reikwijdtebepalingen van de Wbp.
Verwerkingen die zijn onderworpen aan specifieke wetgeving, zoals de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens vallen niet onder de meldplicht. Bij de evaluatie van eerstgenoemde wet zal worden beoordeeld of de meldplicht zich ook tot die wet moet gaan uitstrekken.

4.1.3 Inbreuk op beveiligingsmaatregelen

De meldplicht voor datalekken staat in nauw verband met de beveiligingsverplichting van artikel 13 van de Wbp. Die bepaling verplicht de verantwoordelijke om passende technische en

organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Er is pas sprake van een datalek, wanneer die technische en organisatorische maatregelen niet hebben gefunctioneerd en de persoonsgegevens blootgesteld zijn aan een aanmerkelijk risico van verlies of onrechtmatige verwerking. Hoe dit in praktijk moet worden ingevuld, zal afhankelijk zijn van de omstandigheden. Het is denkbaar dat de verwerking of de daarvan deel uitmakende data het doelwit zijn van hackers die in staat zijn om ook technisch geavanceerde beveiligingsmaatregelen teniet te doen of te omzeilen. Het is ook denkbaar dat een verantwoordelijke slordig omgaat met het beheer van wachtwoorden. Een inbraak of waterschade in het gebouw waarin de verantwoordelijke is gevestigd en die heeft geleid tot blootstelling van persoonsgegevens aan het risico van verlies of onrechtmatige verwerking kan onder omstandigheden ook worden aangemerkt als een inbreuk op de beveiligingsmaatregelen.

4.1.4 Voorkomen van nodeloze meldingen

De effectiviteit van de meldplicht voor datalekken zal snel aan betekenis verliezen wanneer elk denkbaar datalek in aanmerking komt om te worden gemeld. Een meldplicht zonder enige beperking leidt bovendien tot een nodeloze belasting van bedrijfsleven en overheid.
Er zijn twee richtingen denkbaar waarlangs een zinvolle beperking kan worden bereikt. De meldplicht zou beperkt kunnen worden tot bepaalde categorieën gegevens. Daartoe is de Duitse wetgever recent overgegaan. § 42a van het Bundesdatenschutzgesetz beperkt de meldplicht tot bijzondere persoonsgegevens, persoonsgegevens die worden beschermd door een specifiek beroepsgeheim, zoals het medisch of notarieel beroepsgeheim, persoonsgegevens van strafrechtelijke aard en persoonsgegevens met betrekking tot bankrekeningen en kredietkaarten. Een andere beperking van de meldplicht is het gebruik van een algemene formulering die de meldplicht beperkt tot een algemene categorie van relatief zware gevallen. De Oostenrijkse wetgever heeft die keuze gemaakt in § 24 (2a) van het Datenschutzgesetz 2000.
Het Duitse en Oostenrijkse voorbeeld zijn bij wijze van illustratie gegeven. In dit wetsvoorstel wordt noch voor het ene, noch voor het andere model gekozen, maar voor een regeling die aansluit bij de Wbp. De normen van de Wbp zijn algemeen geformuleerd en, behoudens de uitzonderingen op het verbod van de verwerking van bijzondere persoonsgegevens, niet toegesneden op specifieke verwerkingen. Een keuze voor een algemene formulering ter beperking van de meldplicht voor datalekken ligt daarom alleen al uit wetssystematisch oogpunt voor de hand. Een beperking van de meldplicht tot bepaalde categorieën gegevens heeft bovendien als nadeel dat de niet in de wet genoemde categorieën de bescherming door de meldplicht categorisch wordt onthouden, ook wanneer er sprake is van een relatief hoog risico. Zo strekt de hierbovengenoemde Duitse regeling zich niet uit tot bedrijfsvertrouwelijke gegevens of gegevens die worden beschermd door het fiscaal geheim. Daar tegenover staat dat een meer algemene formulering leidt tot meer meldingen. Dat kan echter worden ondervangen door een voorziening om nodeloze meldingen tegen te gaan, in combinatie met voorlichtende maatregelen door het Cbp.
Bij de vraag of aan de meldplicht moet worden voldaan, kan de verantwoordelijke het volgende beslismodel langslopen. Eerst komt de vraag aan de orde of er sprake is van een inbreuk op de getroffen beveiligingsmaatregelen. Is dit het geval, dan komt de vraag aan de orde of de inbreuk tot gevolg heeft gehad dat de verwerkte persoonsgegevens zijn blootgesteld aan een aanmerkelijk risico van verlies of onrechtmatige verwerking. Die laatste stap vergt een beoordeling die zo geobjectiveerd mogelijk moet zijn. Het aanmerkelijk risico dat persoonsgegevens zijn blootgesteld aan verlies of aan onrechtmatige verwerking moet redelijkerwijs aanwezig zijn. Dat moet naar feitelijke omstandigheden van het geval worden vastgesteld. Het risico zal zich bij een geslaagde aanval van hackers eerder voordoen dan bij fysieke schade aan het gebouw waar zich de ICT-apparatuur bevindt waarmee de verwerking plaatsvindt.
Vervolgens moet sprake zijn van een aanmerkelijk risico. Niet elk risico rechtvaardigt immers een melding. Of er sprake is van een aanmerkelijk risico is eveneens afhankelijk van de concrete feiten en omstandigheden. De aard van de inbreuk zal doorgaans van belang zijn bij het bepalen van de grootte van het risico. Het is niet goed mogelijk aan te geven of het verlies van een mobiele telefoon, de diefstal van een laptop of het zoekraken van een geheugenstick wel of geen aanleiding geeft een melding te doen. Of die noodzaak aanwezig is, is afhankelijk van de aard van de data die het betreft en het vermoedelijke risico dat de betrokkene en de verantwoordelijke lopen ingeval van zoekraken of onrechtmatige verwerking.
Tenslotte moet ook aannemelijk zijn dat wanneer het risico op verlies of onrechtmatige verwerking zich verwezenlijkt, dit redelijkerwijs tot nadelige gevolgen voor de persoonsgegevens of de persoonlijke levenssfeer van de betrokkene leidt. Omvang en aard van de verwerking zijn mede bepalend voor de vraag of de verwezenlijking van het risico als nadelig voor persoonsgegevens en de bescherming van de persoonlijke levenssfeer moet worden aangemerkt. Het zoekraken of hacken van de ledenadministratie van een sportvereniging zal doorgaans leiden tot het nodige ongemak voor vereniging en leden, maar zal niet snel aanleiding geven tot een melding bij het

Cbp. De gevolgen van een dergelijk datalek blijven doorgaans beperkt en ook van betrokkenen kan worden gevergd dat zij een zekere mate van risico aanvaarden. Dat is nu eenmaal onlosmakelijk verbonden met het normaal vertrouwen in maatschappelijke verhoudingen. Maar een datalek bij, bijvoorbeeld, de Belastingdienst of de Sociale Verzekeringsbank (SVB) of een commerciële bank of verzekeraar is doorgaans van geheel andere orde. Een datalek bij dergelijke instellingen kan leiden tot financieel nadeel bij de betrokkene of de compromittering van gegevens die beschermd worden door een geheimhoudingsplicht.
Van deze instellingen mag worden verwacht dat zij de grote hoeveelheden gegevens die zij dagelijks verwerken op een professionele wijze beveiligen en dat die beveiliging ook wordt aangepast aan veranderende omstandigheden. De aard van de door de Belastingdienst verwerkte gegevens is ook zodanig dat een datalek kan leiden tot een aanmerkelijke inbreuk op de persoonlijke levenssfeer van de betrokkenen, omdat het belastinggeheim kan worden geschonden. Tenslotte mag van het Cbp worden verwacht dat het boetebeleidsregels zal vaststellen waarmee het college indirect enig houvast kan geven aan de praktijk. Daarin zal ook kunnen worden ingegaan op de invulling van de voorziening om nodeloze meldingen te voorkomen. Vermoedelijk zal het Cbp ook nog aanvullende voorlichting aan de praktijk geven.

4.1.5 Melding aan Cbp en aan betrokkene

In overeenstemming met het nieuwe artikel 11.3a van de Tw is ervoor gekozen om de verantwoordelijke te verplichten de melding zowel aan het Cbp als aan de betrokkene te doen. In het voorgestelde artikel 34a, eerste en tweede lid, van de Wbp is dat geregeld. Met de meldplicht aan het Cbp wordt beoogd het toezicht op potentieel ernstige datalekken te ondersteunen. Het Cbp moet door de verantwoordelijke worden geïnformeerd opdat het Cbp kan beoordelen of een onderzoek of het geven van aanwijzingen noodzakelijk is. Het is zeker geen gegeven dat het Cbp iedere melding laat volgen door een onderzoek of andere maatregelen. Een verantwoordelijke die handelt op de manier die van hem mag worden verwacht treft immers zelf zo spoedig mogelijk de nodige maatregelen om het datalek te dichten en herhaling van het voorval tegen te gaan. De verantwoordelijke zal ook bekend maken wat hij onderneemt. Een melding bij het Cbp zal in die gevallen veelal zonder enige reactie blijven. Het ligt overigens in de rede dat het Cbp deze meldingen zelf wel opslaat, mede om daarover, bijvoorbeeld in het jaarverslag, verantwoording over af te leggen.
Met de meldplicht aan de betrokkene wordt beoogd de betrokkene op de hoogte te stellen van de feitelijke situatie en de consequenties die dat voor zijn belangen heeft. De betrokkene heeft aldus de mogelijkheid nadere informatie te vragen of te beslissen of hij van zijn rechten op inzage, correctie of afscherming gebruik wil maken. In paragraaf 4.1.1 is ingegaan op de verschillen tussen de meldplichten op grond van Wbp en Tw. Op grond van het voorgestelde artikel 34a, achtste lid, van de Wbp moet de verantwoordelijke een overzicht bijhouden van alle inbreuken. Dat betreft ook de inbreuken die wel zijn geconstateerd, maar niet zijn gemeld, omdat zij naar het oordeel van de verantwoordelijke niet waren aan te merken als meldingsplichtige inbreuken. Verder dienen de gegevens die aan het Cbp zijn verstrekt te worden geregistreerd, alsmede de tekst van de kennisgeving die de verantwoordelijke aan de betrokkene doet. Deze protocolplicht ondersteunt het interne en externe toezicht op de gegevensverwerking. Achteraf kan aan de hand van het protocol worden beoordeeld of de inbreuk niet toch had moeten worden gemeld.
Voor organisaties die een functionaris voor de gegevensbescherming hebben aangesteld, ligt het voor de hand dat de functionaris degene is die belast is met de feitelijke uitvoering van de melding namens de verantwoordelijke. Het ligt evenzeer voor de hand dat het Cbp in de gevallen waarin nader contact met de verantwoordelijke nodig is, zich met de functionaris in verbinding stelt.

4.1.6 Inhoud van de melding

De kennisgeving aan het Cbp en betrokkene omvat in het voorgestelde artikel 34a, derde lid, Wbp een aantal gemeenschappelijke elementen. In elk geval worden steeds de aard van de inbreuk, de instanties waar meer informatie kan worden verkregen en aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken gemeld. Bij vermelding van de aard van de inbreuk zal doorgaans met een algemene omschrijving kunnen worden volstaan. Wanneer de betrokkene wil weten waar hij persoonlijk aan toe is, kan hij contact opnemen met de verantwoordelijke. Die moet daartoe in de kennisgeving contactgegevens opnemen. Organisaties die een functionaris voor de gegevensbescherming hebben aangesteld kunnen overwegen dat contact via de functionaris te laten verlopen. Verder dient de verantwoordelijke, ter beperking van de schade die door het mogelijke verlies of de onrechtmatige verwerking kan ontstaan, maatregelen bekend te maken die de betrokkene zelf kan of moet nemen. Gedacht kan worden aan het veranderen van gebruikersnamen en wachtwoorden wanneer deze door de inbreuk mogelijk gecompromitteerd zijn.

Het staat de verantwoordelijke vrij om meer toe te voegen aan de kennisgeving, maar verplicht is dat niet.
De kennisgeving aan het Cbp omvat meer elementen. In het voorgestelde artikel 34a, vierde lid, van de Wbp moeten aan het Cbp meer gegevens, vooral van technische aard, worden gemeld. Dat stelt het Cbp in staat effectief toezicht uit te oefenen. De aanvullende kennisgeving is echter ook in het belang van de verantwoordelijke. Het kan zijn dat bij de kennisgeving melding moet worden gemaakt van technische details die van vertrouwelijke aard zijn. Van het ongecontroleerd prijsgeven van details over de beveiliging van persoonsgegevens kunnen kwaadwillenden immers profiteren. Bedrijven kunnen deze gegevens desgewenst als bedrijfsvertrouwelijk in de zin van artikel 10, eerste lid, onder c, van de Wet openbaarheid van bestuur aanmerken.

4.1.7 Wijze van melden

Ter beperking van de administratieve lasten en nalevingskosten is bewust gekozen voor een zo eenvoudig mogelijke melding. Wel zijn er enkele minimumeisen opgenomen met betrekking tot de inhoud van de melding. Het voorgestelde artikel 34a, vijfde lid, van de Wbp geeft een in het systeem van de Wbp passende afwegingsplicht mee. De verantwoordelijke moet rekening houden met de aard van de inbreuk en de gevolgen ervan. Daarnaast mag hij rekening houden met de omvang van de kring van de betrokkenen en de kosten van de tenuitvoerlegging. Wanneer de inbreuk zich zou beperken tot een verhoudingsgewijs klein aantal betrokkenen, kan de verantwoordelijk ervoor kiezen hen persoonlijk en gericht te benaderen. Wanneer de inbreuk een groot aantal betrokkene treft, ligt naast de gebruikelijke bekendmaking op een website een advertentie in de dagbladen meer in de rede. In Europees verband wordt door het Europees Agentschap voor netwerk- en informatieveiligheid (ENISA) overigens gewerkt aan een geharmoniseerd formulier voor het melden van datalekken. Hoewel de meldingen bij ENISA niet specifiek zien op datalekken waarbij persoonsgegevens worden blootgesteld, is het toch denkbaar dat het formulier ook bruikbaar kan zijn voor de meldplicht die in dit wetsvoorstel is geregeld. Dat formulier kan goede diensten bewijzen bij datalekken met grensoverschrijdende effecten, waarbij samenwerking tussen de toezichthouders van de lidstaten nodig is. Zonodig kan gebruik van dat formulier, of een ander format, bij algemene maatregel van bestuur op grond van artikel 34a, elfde lid, van de Wbp worden voorgeschreven. Dit formulier zal dan alleen gebruikt worden voor de melding aan het Cbp, niet voor de melding aan de betrokkenen.

4.1.8 Uitzonderingen op de meldplicht

Wanneer de verantwoordelijke de moeite heeft genomen de door hem verwerkte persoonsgegevens zodanig te beveiligen dat het redelijkerwijs is uitgesloten dat een datalek kan leiden tot kennisname van persoonsgegevens door onbevoegden, kan de kennisgeving aan de betrokkene achterwege worden gelaten. Het Cbp beoordeelt of dit feitelijk het geval is. Het voorgestelde artikel 34a, zesde lid, van de Wbp geeft als voorbeeld het gebruik van encryptie, maar laat de mogelijkheid open dat andere technieken die een vergelijkbaar beschermingsniveau bieden ook in aanmerking komen. De verantwoordelijke kan zelf in zijn kennisgeving aan het Cbp aangeven dat hij van oordeel is, dat een kennisgeving aan de betrokkene achterwege kan blijven. Echter, bij de beoordelingsruimte die het Cbp krijgt toegekend in artikel 34a, zesde lid, van de Wbp, past dat het Cbp zonodig expliciet kan verlangen dat de verantwoordelijke toch een kennisgeving aan de betrokkene doet. Deze voorziening is opgenomen in het voorgestelde artikel 34a, zevende lid, van de Wbp.
De meldplicht krachtens het voorgestelde artikel 34a geldt niet, indien de verantwoordelijke in zijn hoedanigheid van aanbieder van een elektronische communicatiedienst op grond van artikel 11.3a, eerste en tweede lid, van de Tw al een kennisgeving heeft gedaan. Deze uitzondering op de meldplicht van artikel 34a van de Wbp geldt niet in situaties waarin de verantwoordelijke een ander is dan de aanbieder van de elektronische communicatiedienst bedoeld in artikel 11.3a van de Tw. In een dergelijk geval is een inbreuk gemaakt op zowel de beveiligingsmaatregelen die de verantwoordelijke moet nemen ter uitvoering van artikel 13 Wbp als op de maatregelen die de aanbieder op grond van artikel 11.3 Tw moet nemen. Dan moeten beide partijen een melding doen op grond van artikel 34a Wbp, respectievelijk 11.3a Tw.

4.1.9 Meldingen op grond van de Wet op het financieel toezicht

Op grond van de artikel 3:17 en 4:15 van de Wet op het financieel toezicht (Wft) zijn financiële ondernemingen verplicht hun bedrijfsvoering zodanig in te richten dat deze een beheerste en integere uitoefening van hun bedrijf waarborgt. De wetgever heeft de norm van integere bedrijfsuitoefening vooral gesteld met het oog op het behoud van het vertrouwen in de desbetreffende onderneming en de relevante financiële markten.

Wat betreft de omgang met gegevens, waaronder mede begrepen persoonsgegevens, schrijven artikel 20, tweede lid, van het Besluit prudentiële regels Wft en artikel 30, vierde lid, van het Besluit gedragstoezicht financiële ondernemingen Wft een beveiligingsverplichting voor. Die verplichting verschilt in essentie niet van de verplichtingen gesteld in de artikelen 13 van de Wbp en artikel 11.3 van de Tw.
De artikelen 3:10, derde lid, en 4:11, vierde lid, van de Wft verplicht financiële ondernemingen om aan De Nederlandsche Bank (DNB), onderscheidenlijk de Autoriteit Financiële Markten (AFM), informatie te verstrekken over incidenten die betrekking hebben op de integere bedrijfsuitoefening. Op grond van de artikelen 12 van het Besluit prudentiële regels Wft en 19 van het Besluit gedragstoezicht financiële ondernemingen Wft moeten de ondernemingen die incidenten intern vastleggen.
Het is evident dat de onrechtmatige verwerking van persoonsgegevens in verband met de financiële huishouding van natuurlijke personen tot direct aanwijsbare financiële schade aanleiding kan geven. Als die onrechtmatige verwerking kan worden toerekend aan een financiële ondernemening doordat de beveiligingsverplichting niet goed is nageleefd, dan kan dat het vertrouwen in de desbetreffende onderneming snel aantasten, tenzij op korte termijn de nodige maatregelen worden genomen. Skimmingpraktijken zijn daarvan een voorbeeld. Dergelijke incidenten vallen onder het bereik van de meldplicht. Daarmee is verzekerd dat de bevoegde toezichthouders, DNB en AFM, op de hoogte worden gesteld van datalekken. Deze toezichthouders beschikken bovendien over de nodige instrumenten om zonodig te interveniëren bij de financiële onderneming. In het uiterste geval kan een bestuurlijke boete worden opgelegd.
Verder is het zo dat financiële ondernemingen hun cliënten zo spoedig mogelijk informeren over het incident, wanneer dat gevolgen heeft of heeft gehad voor de desbetreffende cliënt. In gevallen waarin daartoe aanleiding bestaat, wordt de cliënt schadeloos gesteld. In termen van de bescherming van persoonsgegevens zijn de belangen van de betrokkene daarmee afdoende gewaarborgd.
Het stelsel van de Wft voldoet daarmee reeds in vergaande mate aan de uitgangspunten van dit wetsvoorstel. Immers, ook dit stelsel is bij uitstek gericht op het behoud, en waar nodig, herstel van vertrouwen van betrokkenen in verantwoordelijken. Er is dan ook geen aanleiding verandering aan te brengen in dit stelsel door het opleggen van dubbele meldplichten aan de financiële sector. Voorgesteld wordt dan ook om in artikel 34a, tiende lid, van de Wbp een voorziening op te nemen die inhoudt dat de meldplicht niet van toepassing is op ondernemingen voor wie reeds een meldplicht geldt uit hoofde van de Wft.
Er is overigens wel een relevant verschil tussen de meldplichten op grond van dit wetsvoorstel en de meldplichten op grond van de Wft. De geheimhoudingsplichten van de artikelen 1:89 en 1:90 van de Wft laten geen ruimte om meldingen van datalekken door de verantwoordelijke aan de betrokkene op dezelfde wijze te doen als in artikel 34a van de Wbp is voorgeschreven. Die regeling gaat immers uit van een openbare kennisgeving. Dergelijke openbare kennisgevingen in de financiële sector zijn - 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. Waar de praktijk leert dat financiële ondernemingen hun verantwoordelijkheid jegens hun cliënten in rechtstreeks contact met die cliënt nemen, is verzekerd dat het verschil tussen de meldplichten geen nadelige gevolgen voor de betrokkenen heeft.

4.1.9 Delegatiebepaling

In het voorgestelde artikel 34a, elfde lid, van de Wbp is de grondslag opgenomen voor een algemene maatregel van bestuur. In die maatregel kunnen nadere regels worden opgenomen met betrekking tot de inhoud en de wijze van kennisgeving. De meldplicht voor datalekken is een nieuwe regeling waarmee nog weinig ervaring bestaat. Wanneer meer ervaring is opgedaan met de nieuwe regeling kan blijken dat er behoefte bestaat aan aanvullende regels over de kennisgeving. Zekerheid bestaat daarover niet, zodat volstaan kan worden met een bevoegdheid tot het stellen van nadere regels. Een vergelijkbare bepaling is opgenomen in artikel 11.3a, zevende lid, van de Tw. Het ligt in de rede dat wanneer de noodzaak tot het vaststellen van deze nadere regels zich aandient, die regels in één algemene maatregel van bestuur worden opgenomen die zijn grondslag vindt in zowel de Wbp als de Tw.

4.1.10 Verhouding tot het aansprakelijkheidsrecht

Het doen van een kennisgeving aan de betrokkene ontheft de verantwoordelijke op zichzelf genomen 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. Artikel 49 van de Wbp bevat daarvoor een afzonderlijke voorziening die de aansprakelijkheid en de verplichting tot het betalen van schadevergoeding bij de verantwoordelijke legt. De verantwoordelijk kan eventueel regres nemen op een bewerker. Dat wil niet zeggen dat de kennisgeving uit hoofde van het aansprakelijkheidsrecht geen betekenis heeft. 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. Verantwoordelijken doen er daarom goed aan dit bij de afweging om wel of geen kennisgeving aan betrokkenen te doen mee te nemen. Handelt de betrokkene nadat hem een kennisgeving is gedaan niet overeenkomstig de door de verantwoordelijke voorgestelde maatregelen, en vloeit daaruit schade voor de hem voort, dan kan onder omstandigheden sprake zijn van eigen schuld van de betrokkene.

4.1.11 Sanctionering

Overeenkomstig het regeerakkoord wordt voorzien in een robuuste sanctionering voor het nalaten te voldoen aan de meldplicht. Hoewel de voorwaarden waaronder de meldplicht moet worden nagekomen in concreto de nodige beoordeling door het Cbp vergt, blijft het na deze beoordeling een betrekkelijk eenvoudige beoordeling of de meldplicht is nagekomen. In zoverre valt de meldplicht aan te merken als een administratieve verplichting waaraan moet worden voldaan. Het past bij het bestaande stelsel van de Wbp om de overtreding van administratieve verplichtingen te sanctioneren met een bestuurlijke boete. Voorgesteld wordt een maximumboete van € 200.000,=. Dit is een relatief hoog bedrag in verhouding tot de huidige boetemaxima in de Wbp. Dit relatief hoge maximum weerspiegelt het belang dat moet worden gehecht aan het geven van transparantie bij de doorbreking van beveiligingsmaatregelen en het verlies aan vertrouwen dat het gevolg kan zijn van het nalaten van het treffen van de nodige maatregelen.
Naast de bevoegdheden die het Cbp heeft op basis van de Wbp zijn in het wetsvoorstel wijzigingen in de Tw opgenomen die de Cbp soortgelijke bevoegdheden verschaffen bij het toezicht op de naleving en de handhaving van artikel 11.3a van de Tw.

4.1.12 Rechtsbescherming

De toedeling van de meldplicht op grond van twee wetten aan één bestuursorgaan, het Cbp, heeft ook gevolgen voor de rechtsbescherming tegen de door het Cbp vastgestelde sanctiebesluiten. Immers, tegen besluiten van het Cbp staat op grond van de Wbp beroep op de rechtbank en hoger beroep op de Afdeling bestuursrechtspraak van de Raad van State open. Tegen besluiten die op grond van de handhavingsbevoegdheden van de Tw worden vastgesteld, staat in eerste aanleg beroep open op de rechtbank te Rotterdam, en hoger beroep bij het College van Beroep voor het bedrijfsleven. Waar er sprake is van een meldplicht bij één bestuursorgaan, ligt het voor de hand om ook de rechtsbescherming tegen sanctiebesluiten voortvloeiend uit het niet naleven van de meldplicht te uniformeren, en daarvoor aansluiting te zoeken bij het stelsel van de Wbp. Naast de regeling van de rechterlijke bevoegdheid, zijn er ook nog enkele kleine verschillen in enkele regels van procedurele aard tussen Wbp en Tw. In de artikelen II, onderdelen G en H, III en IV zijn daarvoor enkele voorzieningen getroffen.

4.2 Verhouding tot andere meldplichten

De regeling van de meldplicht in dit wetsvoorstel heeft uitsluitend betrekking op het melden van doorbraken van beveiligingsmaatregelen die consequenties hebben of kunnen hebben voor het verlies of de onrechtmatige verwerking van persoonsgegevens. Naast deze meldplichten kent de Tw nog twee andere meldplichten die door dit wetsvoorstel niet worden geraakt. Het betreft de meldplichten van de artikelen 11a.2 en 14.6, tweede lid, van de Tw. De eerstgenoemde meldplicht heeft betrekking op inbreuken op de veiligheid of het verlies van de integriteit van openbare elektronische communicatienetwerken en -diensten, die leiden tot onderbreking van de continuïteit van het netwerk of de dienst. Hierbij moet worden gedacht aan verstoringen van de dienstverlening als gevolg van kabelbreuken door graafwerkzaamheden of uitval van de elektriciteit. Deze gebeurtenissen moeten worden gemeld aan het Agentschap Telecom. De tweede meldplicht betreft de voorbereiding van de relevante aanbieders van openbare elektronische communicatienetwerken en -diensten op de mogelijke verstoring van vitale openbare telecommunicatie-infrastructuur en -diensten in buitengewone omstandigheden. Op grond van de Regeling voorbereiding buitengewone omstandigheden Telecommunicatiewet is aan een groep aangewezen aanbieders een informatieplicht terzake opgelegd. Ook deze meldingen moeten worden uitgebracht aan het Agentschap Telecom. Deze meldplichten blijven gehandhaafd. Zij dienen andere doelen dan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

4.3 Verhouding tot het geldend Europees recht, notificatie

Richtlijn 95/46/EG bevat geen regeling van de meldplicht voor datalekken. Wel bevat artikel 4, derde lid, van richtlijn 2002/58/EG een meldplicht voor datalekken. Die meldplicht geldt echter alleen voor de aanbieders van openbare elektronische communicatiediensten. Voor een meldplicht voor datalekken die zich richt tot elke verantwoordelijke bestaat daarom geen Europeesrechtelijke grondslag. Aangezien het opleggen van een dergelijke verplichting aan een ruimere kring van verantwoordelijken dan die genoemd is in richtlijn 2002/58/EG, betreft het hier een vaststelling van een voorschrift van nationaal recht. Dit voorschrift moet worden aangemerkt als het vaststellen van een regeling met betrekking tot diensten van de informatiemaatschappij in de zin van artikel 1 van *richtlijn 98/34/EG van het Europees Parlement en de Raad van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften (PbEG L 204), zoals gewijzigd bij richtlijn 98/48/EG van het Europees Parlement en de Raad van 20 juli 1998 (PbEG L 217)*.
Dit voorschrift is echter gerechtvaardigd. Een regeling voor de meldplicht van datalekken is een dwingende eis van algemeen belang. De Europese Unie erkent de bescherming van persoonsgegevens als een fundamenteel recht. Dat blijkt uit artikel 8 van het Handvest voor de Grondrechten, artikel 16 van het Verdrag betreffende de werking van de Europese Unie, richtlijn 95/46/EG en richtlijn 2002/58/EG. Het voorschrift is vastgesteld met de bedoeling de betrokkene beter te informeren over belangrijke risico's waaraan zijn persoonsgegevens zijn blootgesteld. Het beoogt tevens gegevens die als gevolg van een verwezenlijking van die risico's in strijd met richtlijn 95/46/EG kunnen worden verwerkt tegen te gaan. Het voorschrift dient daarmee tevens de bescherming van de consument. Het voorschrift voldoet aan de eisen van proportionaliteit, aangezien het zoveel mogelijk vormgegeven is conform de eisen die in artikel 4 van de richtlijn 2002/58/EG, het overigens voldoende ruimte laat om meldingen van gering belang achterwege te laten en voorziet in specifiek toezicht van het Cbp. Met een minder vergaande eis kan in dit geval niet worden volstaan, omdat het achterwege laten van een meldplicht het gevaar oplevert dat de belangen van de betrokkene onvoldoende worden behartigd, en een beperking van de meldplicht tot alleen bepaalde typen van verwerkingen mogelijk discriminatoire effecten heeft. Het voorschrift wordt verder wordt zonder onderscheid toegepast op alle verantwoordelijken in de zin van de Wbp. Overeenkomstig artikel 8 van laatstgenoemde richtlijn is dit wetsvoorstel aan de Europese Commissie genotificeerd.
Afhankelijk van de omstandigheden zal de verantwoordelijke als een dienstverrichter in de zin van artikel 4 van *richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PbEU L 376)* (hierna: Dienstenrichtlijn) kunnen worden aangemerkt. Voor die gevallen geldt dat een meldplicht voor datalekken als een afwijking van het vrij verkeer van diensten kan worden aangemerkt, aangezien de dienstverrichter wordt onderworpen aan een voorschrift van nationale oorsprong dat van invloed is op de wijze van dienstverrichting.
Dit voorschrift is echter gerechtvaardigd in de zin van artikel 16, eerste lid, van de Dienstenrichtlijn. Het voorschrift wordt verder wordt zonder onderscheid toegepast op alle verantwoordelijken in de zin van de Wbp, en zijn ook de uitzonderingen op de verplichting algemeen geformuleerd. Het discriminatieverbod van artikel 16, eerste lid, onder a, van de Dienstenrichtlijn wordt gerespecteerd. Een regeling voor de meldplicht van datalekken is een dwingende eis van algemeen belang die gerechtvaardigd is om redenen van openbare orde. De Europese Unie erkent de bescherming van persoonsgegevens als een fundamenteel recht. Dat blijkt uit artikel 8 van het Handvest voor de Grondrechten, artikel 16 van het Verdrag betreffende de werking van de Europese Unie, richtlijn 95/46/EG en richtlijn 2002/58/EG. Dat blijkt bovendien uit artikel 17, derde lid, van de Dienstenrichtlijn. Het voorschrift is vastgesteld met de bedoeling de betrokkene beter te informeren over belangrijke risico's waaraan zijn persoonsgegevens zijn blootgesteld. Het beoogt tevens gegevens die als gevolg van een verwezenlijking van die risico's in strijd met richtlijn 95/46/EG kunnen worden verwerkt tegen te gaan. Daarmee wordt de fundamentele waarde van de bescherming van persoonsgegevens gediend. Die fundamentele waarde kan geacht worden deel uit te maken van de openbare orde als bedoeld in artikel 16, eerste lid, onder b, van de Dienstenrichtlijn.
Het voorschrift voldoet aan de eisen van evenredigheid als bedoeld in artikel 16, eerste lid, onder c, van de Dienstenrichtlijn. Het voorstel is zoveel mogelijk vormgegeven conform de eisen die in artikel 4 van de richtlijn 2002/58/EG zijn gesteld, het laat overigens voldoende ruimte om meldingen van gering belang achterwege te laten en voorziet in specifiek toezicht van het Cbp. Met een minder vergaande eis kan in dit geval niet worden volstaan, omdat het achterwege laten van een meldplicht het gevaar oplevert dat de belangen van de betrokkene onvoldoende worden

behartigd, en een beperking van de meldplicht tot alleen bepaalde typen van verwerkingen mogelijk discriminatoire effecten heeft.
Overeenkomstig artikel 15, zevende lid, van de Dienstenrichtlijn is dit wetsvoorstel aan de Europese Commissie genotificeerd.

Notificatieprocedure
Het voorstel is van wet is op ... ingevolge *richtlijn 98/34/EG van het Europees Parlement en de Raad van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften (PbEG L 204), zoals gewijzigd bij richtlijn 98/48/EG van het Europees Parlement en de Raad van 20 juli 1998 (PbEG L 217)* alsmede ingevolge *richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PbEU L 376)* voorgelegd aan de Europese Commissie. Naar aanleiding van de reacties van ... wordt het volgende opgemerkt.

4.4 Verhouding tot het strafrecht

In het geval van een datalek kan er een vermoeden zijn van strafbaar handelen. Zo is bijvoorbeeld hacken strafbaar gesteld in artikel 138ab van het Wetboek van Strafrecht. Wanneer er aanwijzingen voor hacken zijn, dan is er ook alle aanleiding om daarvan aangifte te doen bij de politie. Het is niet uitgesloten dat het strafrechtelijk onderzoek aanleiding geeft tot het treffen van opsporingshandelingen als het bewaren van materiaal of het stilleggen van een verwerking. Het belang van het strafrechtelijk onderzoek kan vergen dat een door de verdachte gevolgde unieke werkwijze niet publiekelijk bekend wordt gemaakt, omdat dit het onderzoek zou hinderen.
Ook daarom is in het voorgestelde artikel 34a van de Wbp en in artikel 11.3a van de Tw verzekerd dat de kennisgeving aan het Cbp verschilt van de melding aan de betrokkenen, en dat eerstgenoemde kennisgeving zonodig ook geheel of gedeeltelijk vertrouwelijk kan worden gedaan. Het initiatief daarvoor ligt primair bij de verantwoordelijke. Het kan noodzakelijk zijn dat het Cbp en het openbaar ministerie overleg plegen over hun reacties.

5. Administratieve lasten, nalevingskosten, bestuurlijke lasten, effecten voor de rechtspraak en financiële effecten

5.1 Administratieve lasten en nalevingskosten

De in dit wetsvoorstel opgenomen regeling voor de verruiming van de mogelijkheden tot gegevensverwerking door middel van het beschikbaarstellen van camerabeelden van strafbare feiten aan politie en openbaar ministerie levert geen administratieve lasten en nalevingskosten op. Er is immers geen sprake van informatieverplichtingen van burgers of bedrijven aan overheid. Een belanghebbende heeft het geheel in eigen hand of hij die beelden wel of niet beschikbaar stelt.
De meldplicht voor de doorbrekingen van beveiligingsmaatregelen brengt zowel nalevingskosten als administratieve lasten teweeg. Er moet immers zowel aan betrokkenen, als aan de overheid worden gemeld. Het betreft een geheel nieuwe verplichting. Er is dus geen ervaring beschikbaar waarop kan worden teruggegrepen. Gewerkt moet worden met aannames. Die aannames verschillen deels van de aannames die zijn gebruikt in het in paragraaf 4 van deze memorie genoemde wetsvoorstel tot wijziging van de Tw. Enerzijds is de kring van verantwoordelijken veel groter dan de kring van bedrijven die bij de OPTA zijn ingeschreven. Anderzijds bevat het voorgestelde artikel 34a van de Wbp een voorziening om nodeloze meldingen en bagatelzaken van de meldplicht uit te sluiten.
Aangenomen wordt dat een melding € 8,30 aan nalevingskosten oplevert (melding aan betrokkenen) en eveneens € 8,30 aan administratieve lasten (melding aan het Cbp). Het uurtarief is gewaardeerd op € 50,= en de last per geval geschat op 10 minuten. De gegevens liggen ten grondslag aan het evenbedoelde wetsvoorstel tot wijziging van de Tw (Kamerstukken II 2010/11, 32 549, nr. 3, blz. 26-27). Deze gegevens kunnen zonder bezwaar worden geëxtrapoleerd naar de Wbp. De meldplichten verschillen inhoudelijk immers niet. In een onderzoek van EIM getiteld "Administratieve lasten in het privacydomein, Reductievoorstellen nader bekeken"(Zoetermeer, september 2006) - welk onderzoek mede ten grondslag ligt aan het voorstel van wet houdende *wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen* (Kamerstukken I 2010/11, 31 841, A) - is een schatting gemaakt van het aantal bedrijven dat onder de werking van de Wbp valt. Dat aantal is in het onderzoek vastgesteld op 132.000. Aantekening daarbij verdient dat in Nederland mede als gevolg van een ruimhartig regime voor de vrijstelling van de verplichting om gegevensverwerkingen bij het Cbp aan te melden geen sluitend overzicht bestaat van het aantal bedrijven dat valt onder de reikwijdte van de Wbp. Op dat aantal moet het aantal bedrijven in mindering worden gebracht dat

reeds is onderworpen aan de meldplichten op grond van de Tw en de Wft. De meest recente cijfers, gepubliceerd door de OPTA, de Autoriteit Financiële Markten en De Nederlandsche Bank van het aantal onderneming geeft het volgende beeld. Bij de OPTA staan ongeveer 1000 ondernemingen ingeschreven als aanbieder van een elektronisch communicatienetwerk of elektronische communicatiedienst. Bij de Autoriteit Financiële Markten staan ongeveer 26.500 ondernemingen in zeer uiteenlopende categoriëen ingeschreven. Bij De Nederlandsche Bank gaat het om ongeveer 800 ingeschreven ondernemingen. In totaal betreft het dus 28.300 ondernemingen, zodat de meldplicht uit dit wetsvoorstel betrekking heeft op ongeveer 103.700 ondernemingen.
Het is onmogelijk om op voorhand volledig betrouwbaar te voorspellen in welke gevallen aan de meldplicht uit dit wetsvoorstel gevolg zal moeten worden gegeven. Het gaat niet om de omvang van bedrijven, maar om de grootte van het risico van elke verwerking. Evenmin valt op voorhand te bezien hoe de bagatelregeling zal uitvallen. Wel bestaat het beeld dat datalekken ook in Nederland regelmatig voorkomen. In dit wetsvoorstel wordt daarom aangenomen wordt dat 50% van dat aantal ondernemingen, in totaal 51.850, jaarlijks een melding zal moeten doen. Dat leidt dan tot nalevingskosten van € 430.355,= per jaar en tot administratieve lasten van € 430.355,= per jaar.

5.2 Bestuurlijke lasten en effecten voor de rechtspraak

Dit wetsvoorstel leidt voor het Cbp tot enkele nieuwe bestuurlijke lasten. De meldplicht bij doorbrekingen van beveiligingsverplichtingen leidt, naar thans wordt geschat tot 66.000 meldingen per jaar. Verwacht mag worden dat het overgrote deel van deze meldingen het Cbp geen enkele aanleiding geeft tot een onderzoek of tot handhavingsmaatregelen. Dat betekent dat het Cbp niet meer zal doen dan van de melding kennisnemen en deze gedurende een bepaalde periode zal bewaren. Het valt nog niet te voorzien in hoeveel gevallen de meldingen aanleiding geven tot verdere actie.
De beperking van de kring van verwerkingen die zijn onderworpen aan een voorafgaand onderzoek zal naar alle waarschijnlijkheid niet leiden tot een betekenisvolle vermindering van het aantal aanvragen voor een dergelijk onderzoek. Ook dit valt echter niet goed op voorhand in te schatten. Aangezien het wetsvoorstel tot wijziging van de Tw naar verwachting veel eerder in werking treedt dan het onderhavige voorstel, zal er eerst een situatie ontstaan waarin de OPTA als enig bevoegd bestuursorgaaan meldingen in ontvangst neemt, deze beoordeelt en waar nodig intervenieert. Bij inwerkingtreding van dit wetsvoorstel valt deze taak toe aan het Cbp. Hoewel veel praktische gevolgen op informele wijze tussen Cbp en OPTA geregeld kunnen worden, bijvoorbeeld in een convenant, is het raadzaam voor eventuele rechtsgeschillen naar aanleiding van opgelegde boetes een overgangsbepaling op te nemen.
De consequenties van het wetsvoorstel voor de organisatie van het Cbp zijn dan ook nog niet goed in kaart te brengen. Zoals volgt uit de meergenoemde brief van de eerste ondergetekende aan de voorzitter van de Tweede Kamer der Staten-Generaal van 27 oktober 2011, zullen de eventuele veranderingen in de werklast van het Cbp als gevolg van de introductie van de meldplicht eerst feitelijk moeten worden vastgesteld, voordat een beslissing kan worden genomen over de gevolgen die aan die vaststelling moet worden verbonden.
Het valt uiteraard niet uit te sluiten dat de handhaving van de meldplicht aanleiding geeft tot het opleggen van een sanctie. Een bestuurlijke boete lijkt dan het meest voor de hand liggende middel te zijn. Het Cbp is onafhankelijk, en bepaalt zijn eigen handhavingsbeleid. Niettemin kan ervan worden uitgegaan dat het Cbp na inwerkingtreding van dit wetsvoorstel de praktijk wel enige gelegenheid gunt aan de nieuwe verplichting te wennen, en dat ook het Cbp zich na inwerkingtreding eerst concentreert op de goede gang van zaken bij de afwikkeling van de meldplicht, het beoordelen van meldingen en het plegen van informele interventies bij verantwoordelijken als daar aanleiding toe is. Verder mag van het Cbp worden verwacht dat het, mogelijk pas enige gewenningstijd, boetebeleidsregels vaststelt.
Vooralsnog wordt rekening gehouden met tien boetebesluiten per jaar. Een boetebesluit is doorgaans altijd voorwerp van bezwaar en beroep. Er moet dus rekening worden gehouden met een belasting van de rechtspraak met tien zaken per jaar.

5.3 Gevolgen voor de rijksbegroting

Nader in te vullen na consultatie.

6. Advies en consultatie

Het wetsvoorstel is voor advies voorgelegd aan het Cbp. Daarnaast zijn in een consultatie de volgende organisaties in de gelegenheid gesteld een zienswijze te geven: de Raad voor de rechtspraak, de Nederlandse Vereniging voor Rechtspraak, het College van procureurs-generaal, de

Nederlandse Orde van Advocaten, de OPTA, het Agentschap Telecom, DNB, de AFM, VNO/NCW, ICT Office, de Nederlandse Vereniging van Banken, het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming, Bits of Freedom en de FNV.
Verder is dit wetsvoorstel voorwerp van een internetconsultatie geweest.
PM reactie op adviezen en zienswijzen.

Artikelsgewijs

Artikel I, onderdelen B en C

Artikel 22, vierde lid, van de Wbp bevat de voorwaarden waaronder strafrechtelijke gegevens ten behoeve van derden mogen worden verwerkt, buiten de gevallen waarin die gegevens worden verwerkt door politie, openbaar ministerie en andere ambtenaren met de opsporing van strafbare feiten belast. Voor zover het niet betreft de gevallen waarin de verwerking plaatsvindt door particuliere beveiligingsorganisaties en recherchebureaus die over een vergunning beschikken en verwerkingen binnen een groep in vennootschapsrechtelijke zin, is er slechts één restcategorie van gevallen waarin strafrechtelijke gegevens ten behoeve van derden mogen worden verwerkt. Dit is slechts mogelijk wanneer passende en specifieke waarborgen zijn getroffen en een voorafgaand onderzoek door het Cbp mogelijk is geweest.
In artikel I, onderdeel B, onder 1 en 3, is een wijziging van artikel 22, vierde lid, onder c, van de Wbp opgenomen om de zeer beperkte mogelijkheid tot verwerking van strafrechtelijke gegevens voor andere gevallen beheerst te verruimen. De vereisten tot het treffen van passende en specifieke waarborgen en het voorafgaand onderzoek worden niet meer cumulatief, maar alternatief gesteld. De passende en specifieke waarborgen zullen in een krachtens het nieuwe achtste lid van artikel 22 van de Wbp vast te stellen algemene maatregel van bestuur worden opgenomen. Dat betekent enerzijds dat voor de categorieën van gevallen die in de algemene maatregel van bestuur regeling zullen vinden geen voorafgaand onderzoek door het Cbp meer nodig is, maar anderzijds dat dit onderzoek buiten de geregelde gevallen onverkort nodig blijft. Dat heeft ook tot gevolg dat de gevallen waarin de verwerking van strafrechtelijke gegevens door particulieren plaatsvindt buiten de gevallen die hetzij bij algemene maatregel van bestuur zijn geregeld, hetzij krachtens een verklaring van rechtmatigheid van het Cbp plaatsvindt, onrechtmatig zijn. Het Cbp kan dan handhavend optreden.
In artikel I, onderdeel C, is een corresponderende wijziging van artikel 31 van de Wbp opgenomen. In die bepaling vindt de procedure van het voorafgaand onderzoek regeling. De reikwijdte van die bepaling wordt enigszins beperkt.
In artikel I, onderdeel B, onder 2, is een wijziging opgenomen van artikel 22, zevende lid, van de Wbp. In verband met een grotere rol die particuliere beveiligingsdiensten wordt toebedacht bij de verwerking van strafrechtelijke gegevens kan de behoefte ontstaan die rol nader te omschrijven met algemene regels die in het belang van de bescherming van persoonsgegevens kunnen worden gesteld.

Artikel II, onderdelen A en B

Met deze wijzigingen in hoofdstuk 11 van de Tw wordt beoogd de verantwoordelijkheid voor het in ontvangst nemen van meldingen bij het Cbp te beleggen.

Artikel II, onderdelen C tot en met E

Het Cbp wordt volgens de systematiek van Tw belast met het toezicht op de naleving van de bepalingen met betrekking tot de beveiligingsplichten en de meldplicht. Daartoe strekt de wijziging van artikel 15.1 Tw. Daarnaast krijgt het Cbp de bevoegdheid tot oplegging van een last onder bestuursdwang. Dat wordt geregeld in het nieuwe artikel 15.2, vierde lid, Tw. Deze bevoegdheid brengt in het systeem van de Algemene wet bestuursrecht (Awb) van rechtswege de bevoegdheid tot het opleggen van een last onder dwangsom met zich mee. In het nieuwe artikel 15.4, vierde lid, Tw is voorzien in de bevoegdheid van het Cbp tot oplegging van een bestuurlijke boete bij het niet naleven van de meldplicht. Hetgeen in het algemeen gedeelte van deze memorie in paragraaf 4.1.111 is toegelicht ten aanzien van de toedeling van de boetebevoegdheid in de Wbp is ook van toepassingen ten aanzien van toedeling van dezelfde bevoegdheid in de Tw.

Artikel II, onderdeel G

In paragraaf 4.1.11 van het algemeen gedeelte van deze toelichting is reeds aangegeven dat het rechtsbeschermingsstelsel van de Wbp van toepassing is. In de Wbp is, anders dan in de Tw geen regeling getroffen voor de schorsende werking van een ingesteld verzet tegen de tenuitvoerlegging

van een dwangbevel tot invordering van een bestuurlijke boete. In verband met de toedeling van de boetebevoegdheid aan het Cbp dient te worden uitgesloten dat de schorsende werking van het verzet wel zou bestaan bij besluiten van het Cbp genomen op grond van de Tw, terwijl deze niet bestaat bij bestuurlijke boetes opgelegd op grond van de Wbp. In artikel I, onderdeel G, is daarvoor een voorziening getroffen. Voor bestuurlijke boetes opgelegd door andere bestuursorganen, belast met de handhaving van de Tw blijft de schorsende werking van het verzet onaangetast.

Artikel II, onderdeel H, en artikel III

Deze voorzieningen strekken ertoe de rechtsbescherming tegen sanctiebesluiten van het Cbp op grond van de artikelen 15.2, vierde lid, en 15.4, vierde lid, van de Tw op te dragen aan de rechtbank en de Afdeling bestuursrechtspraak van de Raad van State.

Artikel IV

Het wetsvoorstel tot wijziging van de Telecommunicatiewet (Kamerstukken 32 549) zal naar verwachting eerder in werking treden dan het onderhavige wetsvoorstel. Aangezien dit wetsvoorstel een ander rechtsbeschermingsregime kent dan het systeem van de Telecommunicatiewet, is het noodzakelijk overgangsrecht vast te stellen voor recht om bezwaar te maken of beroep of hoger beroep in te stellen tegen sanctiebesluiten van de OPTA terzake van het nalaten te voldoen aan de meldplicht, alsmede voor het procesrecht dat van toepassing is op de behandeling van de geschillen. Artikel IV bevat daarvoor een voorziening.

De Staatssecretaris van Veiligheid en Justitie,

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

De Minister van Economische Zaken, Landbouw en Innovatie,