W03.12.0306/II

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 AaRvS - juli 12)*

Wij Beatrix, bij de gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het noodzakelijk is de Wet bescherming persoonsgegevens en enige andere wetten te wijzigen om het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving te verruimen en een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens in het leven te roepen;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

VOORSTEL VAN WET

ARTIKEL I

De Wet bescherming persoonsgegevens wordt als volgt gewijzigd:

A

Artikel 14 wordt als volgt gewijzigd:

1. In de eerste volzin van het eerste lid wordt "met betrekking tot de te verrichten verwerkingen" vervangen door: met betrekking tot de te verrichten verwerkingen, en ten aanzien van de melding van een inbreuk op die maatregelen waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op nadelige gevolgen voor de persoonsgegevens die door hem worden verwerkt .

2. Het derde lid komt te luiden:

3. De verantwoordelijke draagt zorg dat de bewerker:

a. de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid;

b. de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13, en,

c. de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplichting tot melding van een inbreuk op de maatregelen, bedoeld in artikel 13, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op nadelige gevolgen voor de persoonsgegevens die door hem worden verwerkt .

3. In het vierde lid wordt "in afwijking van derde lid, onder b." vervangen door: in afwijking van het derde lid, onder b en c.

4. In het vijfde lid wordt "alsmede de beveiligingsmaatregelen als bedoeld in artikel 13" vervangen door: "de beveiligingsmaatregelen, bedoeld in artikel 13, en de verplichting tot melding van een inbreuk op die maatregelen waarvan redelijkerwijs kan

worden aangenomen dat die leidt tot een aanmerkelijk risico op nadelige gevolgen voor de persoonsgegevens die door hem worden verwerkt, .

B

Artikel 22 wordt als volgt gewijzigd:

1. Het vierde lid, onderdeel c, komt te luiden:

c. indien passende en specifieke waarborgen zijn getroffen of de procedure is gevolgd, bedoeld in artikel 31.

2. Het zevende lid komt te luiden:

7. Bij algemene maatregel van bestuur worden regels gesteld met betrekking tot de verwerkingen, bedoeld in het vierde lid, onder a en c. Bij die maatregel kan worden bepaald dat de verwerking slechts plaatsvindt met instemming van een bij die maatregel aan te wijzen bestuursorgaaan of andere autoriteit.

C

In artikel 31, eerste lid, onder c, wordt "anders dan krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus" vervangen door: anders dan op grond van de krachtens artikel 22, zevende en achtste lid, gestelde regels of krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus.

D

Na artikel 34 wordt in hoofdstuk 5 een artikel ingevoegd, luidende:

Artikel 34a

1. De verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op nadelige gevolgen voor de bescherming van persoonsgegevens die door hem worden verwerkt.

2. De verantwoordelijke, bedoeld in het eerste lid, stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in het eerste lid, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

3. De kennisgeving aan het College en de betrokkene omvat in ieder geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

4. De kennisgeving aan het College omvat tevens een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

5. De kennisgeving aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.

6. De kennisgeving aan de betrokkene is niet vereist indien de verantwoordelijke gepaste technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft versleuteld zijn of anderszins onbegrijpelijk zijn gemaakt voor eenieder die geen recht heeft op kennisname van de gegevens.

7. Indien de verantwoordelijke geen kennisgeving aan de betrokkene doet, kan het College, indien het van oordeel is dat inbreuk waarschijnlijk nadelige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, van de verantwoordelijke verlangen dat hij alsnog een kennisgeving doet.

8. De verantwoordelijke houdt een overzicht bij van alle inbreuken. Dit overzicht bevat in elk geval de feiten en de gegevens, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.

9. Dit artikel 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.

10. Het tweede en zevende lid zijn niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht.

11. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving.

E

Na artikel 51 wordt een artikel ingevoegd, luidende:

Artikel 51a

1. Het College is bevoegd om in het belang van een efficiënt en effectief toezicht op de naleving op de verwerking van persoonsgegevens afspraken te maken met andere toezichthouders en daartoe gezamenlijk met deze toezichthouders samenwerkingsprotocollen vast te stellen. Een samenwerkingsprotocol wordt bekendgemaakt in de Staatscourant.

2. Het College verstrekt de toezichthouders, bedoeld in het eerste lid, de gegevens betreffende de verwerking van persoonsgegevens welke zij behoeven voor de uitvoering van hun taak.

3. De toezichthouders, bedoeld in het eerste lid, zijn bevoegd uit eigen beweging en desgevraagd verplicht aan het College de gegevens betreffende de verwerking van persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering en het toezicht op de naleving van deze wet.

4. De in het tweede en derde lid bedoelde gegevensverstrekking vindt niet plaats indien de persoonlijke levenssfeer van de betrokkene daardoor onevenredig wordt geschaad.

F

Artikel 66 wordt als volgt gewijzigd:

1. Voor de tekst wordt de aanduiding "1." geplaatst.

2. Er wordt een lid toegevoegd, luidende:

2. Het College kan aan de verantwoordelijke een bestuurlijke boete opleggen van ten hoogste € 450.000,= ter zake van overtreding van het bij of krachtens artikel 34a bepaalde, alsmede van artikel 5:20 van de Algemene wet bestuursrecht.

ARTIKEL II

De Telecommunicatiewet wordt als volgt gewijzigd:

A

In artikel 11.1 wordt, onder vervanging van de punt aan het slot van onderdeel j door een puntkomma, een onderdeel ingevoegd, luidende:

k. College bescherming persoonsgegevens: het College bescherming persoonsgegevens, bedoeld in de Wet bescherming persoonsgegevens.

B

In artikel 11.3a, eerste, derde, vierde en vijfde lid, wordt "het college" telkens vervangen door: het College bescherming persoonsgegevens.

C

Artikel 15.1 wordt als volgt gewijzigd:

1. Onder vernummering van het derde tot vierde lid wordt een nieuw derde lid ingevoegd, luidende:

3. Met het toezicht op de naleving van het bepaalde bij of krachtens artikel 11.3a zijn belast de bij besluit van het College bescherming persoonsgegevens aangewezen ambtenaren.

2. In de eerste volzin van het vierde lid wordt "eerste en tweede lid" vervangen door: eerste, tweede en derde lid.

3. In het vijfde lid wordt "eerste, tweede en derde lid" vervangen door: eerste, tweede, derde en vierde lid.

D

Artikel 15.2 wordt als volgt gewijzigd:

1. In het tweede lid wordt "artikel 15.1, derde lid" vervangen door: artikel 15.1, vierde lid.

2. Onder vernummering van het vierde en vijfde tot vijfde en zesde lid wordt na het derde lid een lid ingevoegd, luidende:

4. Het College bescherming persoonsgegevens is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van de verplichtingen, gesteld bij of krachtens de in artikel 15.1, derde lid, bedoelde bepalingen.

E

Artikel 15.4 wordt als volgt gewijzigd:

1. Onder vernummering van het vierde, vijfde en zesde lid tot vijfde, zesde en zevende lid wordt na het derde lid een lid ingevoegd, luidende:

4. Het College bescherming persoonsgegevens kan een bestuurlijke boete opleggen van € 450.000,= ter zake van overtreding van de bij of krachtens de in artikel 15.1, derde lid, bedoelde regels, alsmede van artikel 5:20 van de Algemene wet bestuursrecht.

2. In het vijfde lid wordt "artikel 15.1, derde lid" vervangen door: artikel 15.1, vierde lid.

F

In artikel 15.5, eerste en tweede lid, en artikel 15.7, eerste en tweede lid, wordt "artikel 15.1, eerste, tweede, onderscheidenlijk derde lid" telkens vervangen door: artikel 15.1, eerste, tweede, derde, onderscheidenlijk vierde lid.

G

In artikel 15.14 wordt "de bestuurlijke boete" vervangen door: de bestuurlijke boete opgelegd door Onze Minister, het college en de raad van bestuur van de mededingingsautoriteit.

H

Aan artikel 17.1 wordt een lid toegevoegd, luidende:

4. Het eerste, tweede en derde lid zijn niet van toepassing op een besluit van het College bescherming persoonsgegevens op grond van de artikelen 15.2, vierde lid, en 15.4, vierde lid.

ARTIKEL III

Onderdeel 3 van de bijlage bij de Wet bestuursrechtspraak bedrijfsorganisatie komt te luiden:

3. Telecommunicatiewet, met uitzondering van de artikelen 15.2, vierde lid, en 15.4, vierde lid; .

ARTIKEL IV

1. Indien het bij koninklijke boodschap van 24 juli 2010 ingediende voorstel van wet houdende wijziging van de Algemene wet bestuursrecht en aanverwante wetten met het oog op enige verbeteringen en vereenvoudigingen van het bestuursprocesrecht (Wet aanpassing bestuursprocesrecht) (Kamerstukken 32 450) tot wet is of wordt verheven en deel A, artikel I, onderdeel CCCCC, van die wet eerder in werking is getreden of treedt dan artikel III van deze wet, vervalt artikel III van deze wet, en wordt bijlage 2 bij de Algemene wet bestuursrecht als volgt gewijzigd:

In de artikelen 7 en 11 komt onderdeel c, onder 3, van de zinsnede met betrekking tot de *Telecommunicatiewet* telkens te luiden:

c. hoofdstuk 15, met uitzondering van de artikelen 15.2, vierde lid, 15.2a en 15.4.

2. Indien het bij koninklijke boodschap van 24 juli 2010 ingediende voorstel van wet houdende wijziging van de Algemene wet bestuursrecht en aanverwante wetten met het oog op enige verbeteringen en vereenvoudigingen van het bestuursprocesrecht (Wet aanpassing bestuursprocesrecht) (Kamerstukken 32 450) tot wet is of wordt verheven en deel A, artikel I, onderdeel CCCCC, van die wet later in werking is getreden of treedt dan artikel III van deze wet, wordt bijlage 2 bij de Algemene wet bestuursrecht als volgt gewijzigd:

In de artikelen 7 en 11 komt onderdeel c, onder 3, van de zinsnede met betrekking tot de *Telecommunicatiewet* telkens te luiden:

c. hoofdstuk 15, met uitzondering van de artikelen 15.2, vierde lid, 15.2a en 15.4

ARTIKEL V

1. Ten aanzien van de mogelijkheid om bezwaar te maken tegen een besluit van de Onafhankelijke Post en Telecommunicatieautoriteit op grond van de artikelen 15.2 en 15.4 van de Telecommunicatiewet terzake van overtreding van het bepaalde bij of krachtens artikel 11.3a van de Telecommunicatiewet dat is bekendgemaakt voor het tijdstip van inwerkingtreding van deze wet, blijft het oude recht van toepassing.

2. Op de behandeling van een bezwaarschrift tegen een besluit als bedoeld in het eerste lid, blijft het oude recht van toepassing.

3. Ten aanzien van de mogelijkheid om beroep of hoger beroep in te stellen tegen een besluit van de Onafhankelijke Post en Telecommunicatieautoriteit op grond van de artikelen 15.2 en 15.4 van de Telecommunicatiewet terzake van overtreding van het bepaalde bij of krachtens artikel 11.3a van de Telecommunicatiewet dat is bekendgemaakt voor het tijdstip van inwerkingtreding van deze wet, blijft het oude recht van toepassing.

4. Op de behandeling van het beroep en hoger beroep tegen een besluit als bedoeld in het eerste lid, blijft het oude recht van toepassing.

ARTIKEL VI

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Staatssecretaris van Veiligheid en Justitie,

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

De Minister van Economische Zaken, Landbouw en Innovatie,

W03.12.0306/II

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 AaRvS - juli 12)*

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

2.1 Gebruik camerabeelden

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 bij tijd en wijle hoog oploopt, 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.

2.2 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.
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.

2.3 Reacties op ontvangen zienswijzen en adviezen

In de ingewonnen adviezen en zienswijzen, met name die van VNO/NCW-MKB Nederland, ICT Office en Bits of Freedom is gevraagd naar mogelijke meer concreet omschreven doelen van de meldplicht. Die zijn er ook. De meldingen dienen ook ter bescherming van de concrete belangen van betrokkenen. Wanneer er duidelijke aanwijzingen bestaan dat er persoonsgegevens gelekt zijn met behulp waarvan het mogelijk is identiteitsfraude te plegen, kan de verantwoordelijke in zijn melding aan betrokkenen aangeven wat de betrokkene daar zelf tegen kan ondernemen, en welke maatregelen de verantwoordelijke heeft getroffen om dat risico te beheersen. Zijn er creditcardgegevens gelekt, dan ligt het voor de hand dat de betrokkene attent wordt gemaakt op de mogelijkheid zijn creditcard te laten blokkeren door de uitgevende instantie. Na een hack bij een provider voor e-mailservices kan in de melding aan de betrokkene wordt geadviseerd het wachtwoord te wijzigen.
Tegelijk moet met VNO/NCW-MKB Nederland en ICT Office worden erkend dat een 100% veilige informatiemaatschappij niet bestaat, en dat het wetsvoorstel daarin geen verandering brengt. Dat is echter geen reden de voorgestelde maatregelen dan maar achterwege te laten. Wanneer de wetgever redelijke maatregelen kan treffen om de veiligheid van de informatiemaatschappij te verhogen, moet dit niet worden nagelaten. Het is inderdaad zo dat de voorgestelde maatregelen leiden tot een verzwaring van de lasten van verantwoordelijken. Die lasten liggen zeker niet alleen bij het bedrijfsleven. Ook de overheid beschikt over een groot aantal zeer omvangrijke en gevoelige verwerkingen van persoonsgegevens. Te denken valt aan die van de Belastingdienst, de uitvoeringsorganen van de sociale zekerheid en de gemeentelijke basisadministratie persoonsgegevens. Beveiligingslekken in deze verwerkingen kunnen zeer grote gevolgen hebben voor betrokkenen.
VNO/NCW-MKB Nederland en ICT Office hebben met het oog op de beheersbaarheid van de lasten voor het bedrijfsleven die aan de meldplicht verbonden zijn aandacht gevraagd voor de ontwikkeling van positieve prikkels voor bedrijven. In hun visie is het effectiever wanneer de wetgever bedrijven die meer inspanningen leveren hun informatiebeveiliging op orde te brengen, beloont, bijvoorbeeld door middel van vrijstellingen of ontheffingen van meldplichten, in plaats van het confronteren van het complete bedrijfsleven met een mogelijk vergaande verplichting. In het wetsvoorstel is erin voorzien dat de verantwoordelijke die technische beschermingsmaatregelen, zoals cryptografie, treft om persoonsgegevens te beveiligen in elk geval is vrijgesteld van de melding aan de betrokkenen. Aan een algehele vrijstelling van de meldplicht zou gedacht kunnen worden wanneer er sprake zou zijn van een algemeen aanvaarde beveiligingsstandaard waarvan het gebruik een zo grote mate van zekerheid biedt voor de beveiliging van persoonsgegevens dat inbreuken of datalekken vrijwel uitgesloten zouden zijn. Dergelijke standaarden bestaan echter niet.

2.4 Relatie met regeerakkoord

In paragraaf 10 "Veiligheid" van het regeerakkoord "Vrijheid en verantwoordelijkheid" van 30 september 2010 zette het kabinet-Rutte I krachtig in op meer cameratoezicht. In dezelfde paragraaf kondigde 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.
Beide maatregelen vloeien mede voort uit het regeerakkoord. Zij zijn ook inhoudelijk 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. Daarnaast is er uit oogpunt van wetgevingsecoonomie voor gekozen beide onderwerpen gezamenlijk in één wijzigingsvoorstel van de Wbp op te nemen.

2.5 Relatie met de Notitie privacybeleid

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 (Kamerstukken II 2011/12, 32 761, nr. 2). 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.

3. Gebruik van camerabeelden vervaardigd door particulieren

3.1 Algemeen

Cameratoezicht in de WbpCameratoezicht 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.

Camerabeelden als vorm van verwerking van bijzondere persoonsgegevens
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.

Uitzonderingen op het verbod om bijzondere persoooonsgegevens te verwerken
Op dat verbod is 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 verwerken van bijzondere persoonsgegevens ten behoeve van derden
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.

Onvoldoende mogelijkheden om bijzondere persoonsgegevens ten behoeve van derden te verwerken
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. Dit wetsvoorstel beoogt de bereidheid tot investeren langs indirecte weg te bevorderen. In dat verband is het van belang erop te wijzen dat de reikwijdte van het wetsvoorstel beperkt blijft tot het aan derden (door middel van het plaatsen op internet) verstrekken van gegevens die zelf rechtmatig worden verwerkt op grond van artikel 22, tweede lid, onder b, van de Wbp. Het moet dus gaan om een verwerking die

redelijkerwijs kan worden aangemerkt als een bescherming van het *eigen* belang van de verantwoordelijke tegen het gevaar dat uitgaat van strafbare feiten. Aan een verwerking moet een behoorlijke beoordeling van doel en middelen van de verwerking te grondslag liggen. Bij gegevens die afkomstig zijn van een geïnstalleerde bewakingscamera en bijbehorende voorzieningen is dat het geval. Dat is echter niet geval bij camerabeelden van andere aard, zoals camerabeelden vervaardigd met mobiele telefoons door toevallige passanten. Daarop ziet dit wetsvoorstel niet.

Twee nieuwe mogelijkheden voor het verwerken van camerabeelden
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, respectievelijk, het primaat van de overheid bij de opsporing en vervolging van strafbare feiten en het belang van de bescherming van persoonsgegevens veiligstellen.

Betrokkenheid van beveiligingsbedrijven
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.

Mogelijkheden voor de plaatsing van beelden op internet door particulieren
Naast mogelijkheid beveiligingsbedrijven in te schakelen is het denkbaar dat onder omstandigheden ook aan particulieren een wat ruimere mogelijkheid kan worden geboden tot verwerking van camerabeelden, buiten de hierbovengenoemde gevallen waarin dit is toegestaan, zonder dat de omslachtige en langdurige procedure van het voorafgaand onderzoek door 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.

Uitwerking
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. Wat de beveiligingsbedrijven betreft, zal nader worden bezien of aanpassing van de vergunningvoorschriften of de geldende gedragscode op grond van artikel 25 van de Wbp zinvol is. 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. Onder alle omstandigheden blijft het plaatsen van camerabeelden door een burger op internet overigens een eigen verantwoordelijkheid van de desbetreffende burger. Ook wanneer de officier van justitie daarvoor toestemming heeft gegeven. De toestemming van de officier van justitie is een oordeel dat gerelateerd moet worden aan het opsporingsbelang. De plaatsing op internet is een vorm van verwerking van persoonsgegevens waarvoor de verantwoordelijke krachtens de Wbp ook in privaatrechtelijke zin altijd zelf verantwoordelijk blijft.

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 verwerkt 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.

3.3 Reactie op ontvangen adviezen en zienswijzen

College van procureurs-generaal
Het College van procureurs-generaal onderschrijft in zijn advies in belangrijke mate de visie van dit wetsvoorstel op de toepassing van cameratoezicht, ook als het gaat om door burgers vervaardigde beelden. Het College is het eens met de in het wetsvoorstel uiteengezette lijn dat beschikbaar beeldmateriaal zo snel mogelijk ter beschikking moet worden gesteld aan de politie.
Het College vraagt zich echter af of de voorgestelde regeling wel meerwaarde biedt ten opzichte van hetgeen de Aanwijzing opsporingsberichtgeving zelf al biedt aan de praktijk. De Aanwijzing voorziet immers in de mogelijkheid dat de politie onder de verantwoordelijkheid van het openbaar ministerie de beelden publiceert met toevoeging van relevante contextuele informatie. Ook wordt nu al gebruik gemaakt van billboards en beeldschermen om de aandacht van het publiek voor de opsporing van verdachten te vragen in samenwerking met stadiondirecties en winkeliersverenigingen. Het wetsvoorstel is niet bedoeld om afbreuk te doen aan de bestaande praktijk. Het is juist de bedoeling de bestaande praktijk aan te vullen voor de gevallen waarin de inspanningen van politie en justitie alleen misschien niet het meest optimale resultaat kunnen bereiken. Het is niet ondenkbaar dat in een individueel geval bij een gerichte inspanning van een burger in de eigen omgeving en de context die hij zelf het beste kent, meer informatie over een strafbaar feit naar voren kan komen dan wanneer dit achterwege wordt gelaten.
Het College vraagt terecht naar de eindverantwoordelijkheid van de door een burger verspreide beelden. Die eindverantwoordelijkheid ligt inderdaad bij de burger zelf. Die verantwoordelijkheid omvat de verantwoordelijkheden die de Wbp op de burger legt, zoals het gehoor geven aan verzoeken om inzage, correctie of afscherming. Die verantwoordelijkheid omvat ook de civielrechtelijke aansprakelijkheid.
Het College vraagt de aandacht voor de toename van de werklast. Het meent dat er sprake zal zijn van een forse toename daarvan. In de eerste plaats wijzen wij erop dat het wetsvoorstel niet betrekking heeft op alle denkbare camerabeelden. Het kan binnen context van artikel 22 van de Wbp uitsluitend betrekking hebben op camerabeelden afkomstig van particuliere bewakingscamera's, en niet van alle beelden die min of meer spontaan met mobiele telefoons, tablets, etc. zijn vervaardigd. Alleen camerabeelden afkomstig van vooraf geïnstalleerde bewakingscamera's kunnen redelijkerwijze worden aangemerkt als getroffen maatregelen voor de verwerking van strafrechtelijke gegevens ter bescherming van het eigen belang in de zin van artikel 22, tweede lid, onder b, van de Wbp. In de tweede plaats mag van politie en justitie worden verwacht dat in het kader van de aangifte van strafbare feiten aangeboden camerabeelden in alle gevallen ook op

bruikbaarheid voor de opsporing worden beoordeeld wanneer dit voorstel van wet niet zou zijn opgesteld, en dat in dat kader een goede belangenafweging wordt verricht, zoals de Aanwijzing overigens voorschrijft. De extra werklast zit dan in het expliciet verlenen van toestemming aan de betrokken burger. Wij menen dat de extra werklast die daaruit voortvloeit overzienbaar zal zijn.
Van meer principiële aard is de afweging van het College dat de opsporing en vervolging van strafbare feiten exclusief aan de overheid is toebedeeld en dat dit mede strekt ter bescherming van de slachtoffers. Het is volgens het College niet ondenkbaar dat het op de burger zelf kan terugslaan wanneer hij beelden publiceert van strafbare feiten die jegens hem zijn gepleegd. Het kan inderdaad in individuele gevallen niet worden uitgesloten dat dit risico aanwezig is. Ook daarom behoort een burger toestemming van de officier van justitie te hebben voor publicatie van de beelden. Wanneer er een aanwijzing is dat dit risico aanwezig is, behoort die toestemming te worden geweigerd. Tenslotte bepleit het College om in het Wetboek van Strafvordering een regeling op te nemen om camerabeelden vormvrij door een opsporingsambtenaar te vorderen. Dit voorstel achten wij een waardevolle suggestie. Het wordt nadrukkelijk in nadere overweging genomen. Uitwerking daarvan vereist echter een afzonderlijke afweging die niet in de context van dit wetsvoorstel kan plaatsvinden.

College bescherming persoonsgegevens
Het Cbp staat niet afwijzend ten opzichte van dit onderdeel van het wetsvoorstel. Het Cbp vraagt aandacht voor drie vraagstukken.
Het Cbp vraagt zich af welke instantie tot handhaving moet overgaan wanneer een burger buiten toestemming van justitie beelden op internet plaatst. Er is dan sprake van het verwerken van gegevens in strijd met de Wbp. Het Cbp is bevoegd daartegen handhavingsmaatregelen te treffen.
Daarnaast vraagt het Cbp naar de gevolgen van plaatsing van beelden op internet, en dan met name de verdere verwerking van de beelden door derden. Bij deze vraagstukken moet inderdaad worden stilgestaan. De algemene maatregel van bestuur die de voorwaarden voor plaatsing zal bevatten, zal daarom ook worden voorzien van maatregelen als een publicatietermijn en inspanningsverplichting de gepubliceerde beelden weer te doen verwijderen. Het Cbp vraagt tenslotte naar de mogelijkheid advies over deze algemene maatregel van bestuur te kunnen uitbrengen. Dat zal gebeuren, aangezien deze maatregel valt onder het bereik van artikel 51, tweede lid, van de Wbp.

Nederlandse Vereniging voor Rechtspraak
De Nederlandse Vereniging voor Rechtspraak (NVvR) stelt zich op het standpunt dat de inbreuk die wordt gemaakt op de persoonlijke levenssfeer onvoldoende in de wet is verankerd, doordat de voorwaarden worden gedelegeerd naar het niveau van de algemene maatregel van bestuur. De NVvR acht dit temeer van belang nu de plaatsing op internet met zich brengt dat beelden uit de macht van de verantwoordelijke raken en vraagt zich af hoe de effecten daarvan zich verhouden tot de onschuldpresumptie. Daarnaast vraagt de NVvR zich af of de handhaving van de voorgestelde bepaling zaak is van het Cbp of dat dit in het strafproces aan de orde moet komen.
De rechtvaardigingsgronden voor het verwerken van strafrechtelijke gegevens door de overheid en door particulieren zijn uitgewerkt in artikel 22 van de Wbp. De Wbp bevat algemeen-abstract geformuleerde normen die niet zijn uitgewerkt naar concrete verwerkingen van persoonsgegevens. Voor zover daar behoefte aan bestaat zal dat moeten gebeuren door deze normen nader uit te werken in een algemene maatregel van bestuur. Dat is in het systeem van de Wbp overigens niet de regel, maar de uitzondering. De regel is dat de uitwerking in concreto plaatsvindt door feitelijk handelen van de verantwoordelijke. Dat er bij algemene maatregel van bestuur regels worden gesteld is dus een aanvullende waarborg, juist ter beveiliging van de belangen waar de NVvR terecht op wijst. Niettemin is dit aanleiding geweest het wetsvoorstel aan te passen door in de delegatiegrondslag het toestemmingsvereiste te expliciteren. De NVvR vraagt terecht aandacht voor de effecten van het plaatsen op internet. Bij de bespreking van het advies van het Cbp gingen wij daar al op in. De handhaving van de Wbp is en blijft

primair zaak van het Cbp. Uiteraard kan niet worden uitgesloten dat zich in een strafproces een keer de vraag zal voordoen of het gebruik van camerabeelden voor het bewijs van een strafbaar feit geoorloofd is, hetzij omdat de inbreuk op de persoonlijke levenssfeer van de op de beelden voorkomende personen in concreto te groot zou zijn, hetzij omdat de voorwaarden voor de verwerking niet zijn nageleefd. Het is dan aan de strafrechter om daarover te beslissen.

Nederlandse Orde van Advocaten
De algemene raad van de Nederlandse Orde van Advocaten (NOvA) beschouwt de voorgestelde regeling uit het oogpunt van verplaatsing van het toezicht van het Cbp naar het openbaar ministerie. NOvA ziet het wegvallen van het toezicht van het Cbp als een verlies, omdat dan onvoldoende gewaarborgd is dat het specifieke belang van de bescherming van de persoonlijke levenssfeer in de te maken afweging aan de orde komt. Wij menen dat die visie onvoldoende recht doet aan de bedoeling van het wetsvoorstel. Die is om goed afgewogen ruimte te bieden aan particulieren om ter beveiliging van hun rechtmatige belangen strafrechtelijke persoonsgegevens te verwerken. Het toezicht van het Cbp blijft bestaan, de toestemming van de officier van justitie is juist een extra waarborg. NOvA wijst op de mogelijkheid de procedure van artikel 31 Wbp te bekorten. Dat laatste is bezwaarlijk. De procedure van artikel 31 van de Wbp is niet toegesneden op de beoordelingen van zeer kleinschalige verwerkingen als de beoordeling van camerabeelden die doorgaans niet meer dan één of enkele minuten aan relevant materiaal bieden, maar op verwerkingen met een permanent of anderszins langduriger of grootschaliger karakter. Voor de beoordeling daarvan is enige tijd nodig.

Vakbeweging, ondernemers en overige reacties
De FNV vraagt om aandacht voor het meewegen van gevoelens van angst voor agressie en geweld bij het personeel van winkelbedrijven die slachtoffer zijn geworden van gewelddadige overvallen voorafgaand aan elke beslissing tot verspreiding van de camerabeelden, ongeacht de grondslag daarvan. Wij hebben begrip voor dit standpunt. Dat belang behoort dan ook mee te wegen bij dergelijke beslissingen. Dat wordt voldoende gewaarborgd door de Aanwijzing en de toestemmingsregeling. De FNV heeft echter bezwaren tegen de verwerking van strafrechtelijke persoonsgegevens door particulieren buiten het thans op grond van de Wbp geldende kader daarvoor. Het gaat er bij deze rechtvaardigingsgrond voor de verwerking van strafrechtelijke persoonsgegevens vooral om dat de gegevensbeschermingswetgeving goed moet worden afgewogen tegen het belang dat particulieren zelf in staat moeten worden gesteld hun eigen belangen te beschermen en het belang van de samenleving dat de verwerking van strafrechtelijke persoonsgegevens niet zover gaat dat het primaat voor opsporing en vervolging van strafbare feiten van de overheid wezenlijk wordt beïnvloed. Dat evenwicht is in dit wetsvoorstel voldoende verzekerd.
Een positieve reactie is uitgebracht door VNO/NCW - MKB Nederland. Ook ontvingen wij positieve reacties uit de internetconsultaties, met name uit de kring van exploitanten van garagebedrijven en benzinestations, bedrijven die veelvuldig het slachtoffer zijn van gewelddadige overvallen. Overigens ontvingen wij in de internetconsultatie ook enige sterk afwijzende reacties van individuele burgers op dit onderdeel van het wetsvoorstel.

4. Meldplicht datalekken

Uitvoering regeerakkoord
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 van het kabinet-Rutte I "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 F, en II, onderdeel E, van het wetsvoorstel.

4.1 Nieuwe voorziening in de Wet bescherming persoonsgegevens

4.1.1 Verhouding Wet bescherming persoonsgegevens en Telecommunicatiewet

Eén toezichthouder voor meldplicht datalekken
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.
Aanbieders van openbare 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

[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.

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 € 450.000,=.

Onderscheid in meldplichten
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 openbare 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.
De begrippen van de Tw verschillen echter van de begrippen van de Wbp. Dat brengt met zich dat in het voorgestelde artikel 34a Wbp verplichtingen worden gelegd op de verantwoordelijke in de zin van de Wbp, en dat de betrokkene in de zin van de Wbp aanspraken krijgt. In artikel 11.3a van de Tw zijn de verplichting gericht tot de aanbieder van een openbare elektronische communicatiedienst in de zin van die wet, en komt het begrip betrokkene niet voor.
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 4.1.5 wordt toegelicht. Hoewel die voorziening is opgenomen is het voorgestelde artikel 34a, eerste lid, van de Wbp, waar een meldplicht van de verantwoordelijke 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 is ook opgenomen 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.

Samenwerking toezichthouders
De voorgestelde voorziening heeft consequenties voor de samenwerking tussen Cbp en OPTA. 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 OPTA voor wederzijdse informatievoorziening ook enkele organisatorische voorzieningen treffen. Dat blijft aan de OPTA en het Cbp om te bepalen. Wel is in artikel I, onderdeel E, van het wetsvoorstel, mede naar aanleiding van het advies van het Cbp, voorzien in een wettelijke grondslag voor deze samenwerkingsrelaties. Voor de OPTA bestaat die grondslag al in artikel 18.3 van de Tw. 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.

4.1.2 Voorstel voor een Algemene verordening gegevensbescherming

Op 25 januari 2012 heeft de Europese Commissie een voorstel gepresenteerd voor een Algemene verordening gegevensbescherming (COM (2012)11 def.). Deze verordening zal richtlijn 95/46/EG gaan vervangen. De artikelen 31 en 32 van de ontwerpverordening bevatten een algemene regeling voor een meldplicht datalekken. Mede naar aanleiding van het advies van Cbp is opnieuw overwogen of de regeling van dit wetsvoorstel niet volledig moet worden toegesneden op die van de ontwerpverordening. Ook in de zienswijzen van andere organisaties is daarop aangedrongen, zoals VNO/NCW-MKB Nederland en ICT-Office. Daarvan wordt afgezien. De regeling van de meldplicht in de ontwerpverordening geeft in dit stadium nog te veel aanleiding tot vragen over de reikwijdte van de daarin opgenomen verplichtingen en de invulling van de daarbij in acht te nemen voorwaarden. Het is nog te prematuur om ervan uit te gaan dat de Europese wetgever met een redelijke mate van zekerheid regeling overeenkomstig het voorstel zal vaststellen. Naar verwachting zal het bovendien nog geruime tijd duren voor de ontwerpverordening wordt vastgesteld. Toch is het advies van het Cbp aanleiding geweest het aanvankelijke voorstel voor artikel 34a van de Wbp tekstueel zo nauw mogelijk te laten aansluiten bij artikel 11.3a van de Tw. Artikel 4, derde lid, van richtlijn 2002/58/EG is niet alleen de bepaling die in artikel 11.3a van de Tw wordt geïmplementeerd, maar ligt ook ten grondslag aan de artikelen 31 en 32 van de ontwerpverordening.

4.1.3 Verantwoordelijke en bewerker

Het voorgestelde artikel 34a van de Wbp richt zich tot de verantwoordelijke. De verantwoordelijke is immers krachtens artikel 13 van de Wbp gehouden de nodige beveiligingsmaatregelen te treffen. Ook overigens vloeit uit de systematiek van de Wbp voort 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 artikel 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. Het Nederlands Genootschap voor Functionarissen voor de Gegevensbescherming (NGFG) vraagt in zijn zienswijze aandacht voor de noodzaak om de nodige instrumenten beschikbaar te stellen die de verantwoordelijke in staat stellen op de bewerker meer invloed uit te oefenen. Dit is echter geen taak voor de wetgever. De rechtsbetrekking tussen verantwoordelijke en bewerker is primair van privaatrechtelijke aard. In de bewerkersovereenkomst zullen verantwoordelijke en bewerker daarover afspraken moeten maken.
Verwerkingen die zijn onderworpen aan specifieke wetgeving, zoals de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens vallen niet onder de meldplicht. Naar aanleiding van de zienswijze van de NOvA kunnen wij aangeven dat na de evaluatie van de Wet politiegegevens zal worden beoordeeld of ook in die wet een meldplicht voor datalekken moet worden opgenomen.

4.1.4 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, waterschade of blikseminslag 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. Onder omstandigheden, want de meldplicht geldt niet wanneer voorzieningen van algemene aard die niet specifiek zijn gericht op de beveiliging van persoonsgegevens worden aangetast.
Bits of Freedom heeft in zijn zienswijze een aanmerkelijk verdergaande reikwijdte van de meldplicht bepleit. Bits of Freedom bepleit elk datalek onder de meldplicht te brengen, wanneer dit in verband kan worden gebracht met elke vorm van ongeoorloofde toegang. Het is zeker zo dat ongeoorloofde toegang kan leiden tot datalekken, die aanleiding behoren te zijn voor het naleven van de meldplicht. Hacken is daarvan het meest aansprekende voorbeeld, maar ook de nalatige omgang met wachtwoorden of vergelijkbare voorzieningen in een werkomgeving. Toch wordt de suggestie van Bits of Freedom niet gevolgd. In de praktijk zal ongeoorloofde toegang moeilijk te onderscheiden zijn van het oneigenlijke gebruik of misbruik maken van gegevens na op zichzelf geoorloofde toegang. 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.

4.1.5 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 en de Tw. 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.
Dat lijkt te prefereren boven een meldplicht die beperkt zou zijn voor alleen "zware gevallen", zoals bepleit is door ICT Office.
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 op nadelige gevolgen voor de persoonsgegevens die door hem worden verwerkt. Die nadelige gevolgen kunnen zich dan vooral voordoen in de vorm van verlies of onrechtmatige verwerking. Tegen die nadelen wil artikel 13 van de Wbp bescherming bieden. Die laatste stap vergt een beoordeling die zo geobjectiveerd mogelijk moet zijn. Het aanmerkelijk risico dat persoonsgegevens zijn blootgesteld aan nadelige gevolgen in de vorm van verlies of 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 aanmerkelijk risico op verlies of onrechtmatige verwerking zich verwezenlijkt, dit redelijkerwijs tot nadelige gevolgen voor 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 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 tot 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.
De voorziening voor het voorkomen van nodeloze meldingen is een essentieel onderdeel van dit wetsvoorstel. Om die reden is het advies van het Cbp om deze voorziening in de vorm van een vrijstellingsregeling te delegeren naar het niveau van de algemene maatregel van bestuur en van die delegatiegrondslag pas gebruik te maken nadat enig ervaring met de meldplicht is opgedaan niet overgenomen.

4.1.6 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 geen gegeven dat het Cbp iedere melding laat volgen door een onderzoek of andere maatregelen. Of een onderzoek en verdere maatregelen volgen, is afhankelijk van de omstandigheden. Het Cbp zal de ingekomen meldingen moeten bezien en daarop reageren in overeenstemming met de door het college zelf gestelde prioriteiten. Verder geldt dat een verantwoordelijke die handelt op de manier die van hem mag worden verwacht zelf zo spoedig mogelijk de nodige maatregelen treft 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. Het NGFG wijst er in zijn zienswijze terecht op dat het voor de hand ligt dat een melding aan het Cbp vergezeld gaat van een melding aan de functionaris voor de gegevensbescherming, indien deze is aangesteld.
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. Het is voor de verantwoordelijke van belang dit protocol goed bij te houden. Mocht de toezichthouder achteraf vragen hebben aan de verantwoordelijke, dan kan de laatste aan de hand van zijn protocol aantonen wat hij heeft geconstateerd en welke maatregelen hij heeft genomen. 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 is uitsluitend bedoeld voor de ondersteuning het interne en externe toezicht op de gegevensverwerking. Zo kan bijvoorbeeld achteraf aan de hand van het protocol door de toezichthouder worden beoordeeld of een geconstateerde, maar niet gemelde inbreuk toch had moeten worden gemeld. Het protocol heeft niet de functie van een openbaar register. Het belang bij het vertrouwelijk blijven van details met betrekking tot de beveiliging van de gegevensverwerking en de daarmee gemoeide investeringen staat daaraan in de weg. De aanbeveling van Bits of Freedom om dit protocol juist wel openbaar te maken wordt dan ook niet gevolgd.
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.
De suggestie van Bits of Freedom om elk datalek onder alle omstandigheden ook aan de betrokkene te melden wordt niet gevolgd. Stellig zou dat leiden tot maximale transparantie, maar dat belang moet worden afgewogen tegen het belang van het beheersen van de lasten van de verantwoordelijke. Dat heeft geleid tot bovenvermelde belangenafweging.

4.1.7 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, al doet dat niets af aan de verantwoordelijkheid van de verantwoordelijke, zoals het NGFG terecht in haar zienswijze stelt. 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 expliciet als bedrijfsvertrouwelijk in de zin van artikel 10, eerste lid, onder c, van de Wet openbaarheid van bestuur aanmerken. Er is dan sprake van een behoorlijk niveau van bescherming van die informatie. Er is dan ook geen noodzaak over te gaan tot een wettelijke voorziening die deze meldingen principieel steeds als vertrouwelijk aanmerkt, zoals VNO/NCW-MKB Nederland en ICT Office hebben bepleit. Anders dan het Agentschap Telecom adviseert, wordt niet voorzien in een verplichting tot een nadere melding wanneer de oorzaak van het incident is achterhaald en de gebreken zijn verholpen. Of een dergelijke mededeling opportuun is, is aan de betrokken instelling of bedrijf overgelaten.

4.1.8 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 verantwoordelijke 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, zoals het Cbp suggereert. Dit formulier zal dan alleen gebruikt worden voor de melding aan het Cbp, niet voor de melding aan de betrokkenen.
Het advies van Cbp en de zienswijze van VNO/NCW-MKB Nederland, ICT Office en het NGFG om voor het tijdstip van de melding een gefixeerde tijdslimiet te hanteren wordt niet gevolgd. De maatstaf onverwijld wordt gehandhaafd om de aansluiting bij de Tw te handhaven. Bovendien geeft het de verantwoordelijke enige gelegenheid om onderzoek te doen naar de inbreuk, te overwegen welke maatregelen hij aanbeveelt en de manier waarop hij communiceert met Cbp en betrokkenen.

4.1.9 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 voorgestelde artikel 34a, zesde lid, van de Wbp verwijst naar het gebruik van encryptie, maar laat de mogelijkheid open dat andere technieken die een vergelijkbaar beschermingsniveau bieden ook in aanmerking komen. Naar aanleiding van een suggestie van Bits of Freedom merken wij op dat het wetsvoorstel geen maatstaven bevat waaraan de encryptie moet voldoen. Dat past bij het techniekneutrale karakter van de Wbp. Naar aanleiding van het advies van het Cbp en de zienswijzen van VNO/NCW-MKB Nederland en het NGFG is een voorafgaand oordeel van het Cbp over de kwaliteit van de encryptie geschrapt. Zodoende blijft de verantwoordelijke in staat zelf het beveiligingsniveau vorm te geven.
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, 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 openbare 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 openbare 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.

4.1.10 Meldingen op grond van de Wet op het financieel toezicht

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 consultatieversie te ruim was. In die versie hoefde een financiële onderneming die een incident als bedoeld in de Wft[2] 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 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.
Er wordt dus voor gekozen om de meldplicht van het onderhavige artikel ook van toepassing te laten 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 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.
In het kader van de administratieve lasten voor financiële onderneming, 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. 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

[2] *Incident:* gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de desbetreffende financiële onderneming (artikel 1 van het Besluit prudentiële regels Wft en artikel 1 van het Besluit Gedragstoezicht financiële ondernemingen Wft).

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 datalekken, ook al leidt dat in een enkel geval tot een dubbele meldplicht voor financiële ondernemingen.

4.1.11 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.

4.1.12 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.
Wanneer het Cbp op grond van artikel 34a, zevende lid, van de Wbp een verantwoordelijke de aanwijzing geeft dat alsnog een melding aan de betrokkenen wordt gedaan, betekent dit niet als vanzelfsprekend dat daardoor bepaalde verantwoordelijkheden en aansprakelijkheden overgaan naar het Cbp, zoals VNO/NCW-MKB Nederland vraagt. De normale regels van de toezichthoudersaansprakelijkheid worden daardoor niet beïnvloed.

4.1.13 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 en

verplichtingen waarvan de handhaving kan plaatsvinden zonder de noodzaak van een gedetailleerde nadere invulling van de onderliggende materiële normen door de toezichthouder,te sanctioneren met een bestuurlijke boete. Voorgesteld wordt een maximumboete van € 450.000,= (artikel I, onderdeel F en artikel II, onderdeel E). Dit is een hoog bedrag in verhouding tot de huidige boetemaxima in de Wbp. Dit 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. Mede naar aanleiding van de adviezen van het Cbp en de OPTA is besloten het boeteniveau zoveel mogelijk in overeenstemming te brengen met het boeteniveau van de Tw. Het in paragraaf 4.1.1 toegelichte voorstel voor een Algemene verordening gegevensbeschermingsrecht kent overigens een aanzienlijk hoger boetemaximum voor hetzelfde vergrijp.
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.
In veel ontvangen zienswijzen, met name uit de internetconsultatie, en in de adviezen van het Cbp, het NGFG is erop aangedrongen ook de overtreding van artikel 13 Wbp - de beveiligingsverplichting - te sanctioneren. Dit alternatief is nadrukkelijk overwogen. Het heeft als voordeel dat beveiliging als aspect van de bescherming van persoonsgegevens integraal wordt aanpakt. Daar staat echter tegenover dat artikel 13 van de Wbp een algemeen-abstract geformuleerde norm is. De handhaving van dergelijke normen vraagt afzonderlijke aandacht uit hoofde van artikel 7 van het Europees Verdrag ter bescherming van de rechten van de mens en de fundamentele vrijheden, vooral op het punt van het lex certa beginsel en de kwestie van de voorzienbaarheid van overtredingen. Dit raakt niet alleen artikel 13 van de Wbp, maar feitelijk de hele vraag naar de verbreding van de handhaving van de materiële normen van de Wbp en een beantwoording van de vraag welke bevoegdheden het Cbp behoeft voor een sterker handhavingsniveau. Een dergelijke stap vergt een veel verdergaande motivering dan in het kader van dit wetsvoorstel kan worden gegeven. Dit vraagt een afzonderlijke afweging in een afzonderlijk wetsvoorstel.
Voorgesteld wordt om ook het niet naleven van de medewerkingsplicht van artikel 5:20 van Algemene wet bestuursrecht met dezelfde boete te bedreigen. Dit betreft dan ook het niet naleven van de medewerkingsplicht in gevallen van onderzoek naar andere overtredingen dan artikel 34a van de Wbp.

4.1.14 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, IV en V 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 geen verplichting. 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 € 16,60 aan nalevingskosten oplevert (een melding aan betrokkenen en het bijhouden van een protocol, elk gewaardeerd op € 8,30), en € 8,30 aan administratieve lasten (melding aan het Cbp). Die bedragen zijn gebaseerd op een uurtarief van € 50,= en een last per geval van 10 minuten. Laatstbedoeld gegeven ligt 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 de wet van 26 januari 2012 *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* (Stb. 33) - is een schatting gemaakt van het aantal bedrijven en overheidsinstellingen 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 over het aantal ondernemingen dat aan het toezicht van dezeinstellingen is onderworpen geeft het volgende beeld. Bij de OPTA staan ongeveer 1000 ondernemingen ingeschreven als aanbieder van een openbaar elektronisch communicatienetwerk of openbare elektronische communicatiedienst. Bij de Autoriteit Financiële Markten staan ongeveer 26.500 ondernemingen in zeer uiteenlopende categorieën ingeschreven. Bij De Nederlandsche Bank gaat het om ongeveer 800 ingeschreven ondernemingen. In totaal betreft het dus 28.300 ondernemingen, zodat de meldplichten op grond dit wetsvoorstel betrekking hebben op ongeveer 131.000 ondernemingen en instellingen waar het de melding aan het Cbp betreft en ongeveer 103.700 ondernemingen en instellingen waar het de meldplicht aan de betrokkenen betreft.
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 het aantal ondernemingen jaarlijks een melding zal moeten doen.
Uitgewerkt voor de administratieve lasten (de melding aan het Cbp) levert dit op dat 50% van 131.500 ondernemingen (namelijk 132.500, verminderd met 1000 ondernemingen die reeds onder de Tw vallen) jaarlijks een melding doet aan het Cbp. Dit levert € 543.650,= jaarlijks aan administratieve lasten op.
Uitgewerkt voor de nalevingskosten, gemoeid met het doen van een melding aan de betrokkene levert dit op dat 50% van 103.700 ondernemingen (namelijk 132.000, verminderd met 1000 ondernemingen die onder de Tw vallen, en 27.300 die onder de Wft vallen) jaarlijks een melding doet. Dit levert € 430.355,= jaarlijks aan nalevingskosten op.
Uitgewerkt voor de nalevingskosten, gemoeid met het bijhouden van een protocol levert dit op dat 50% van 131.500 ondernemingen (namelijk 132.000 verminderd met 1000 ondernemingen die reeds onder de Tw vallen) een protocolbijwerking moet doen. Dit levert € 543.650,= jaarlijks aan nalevingskosten op. De totale jaarlijkse nalevingskosten worden geraamd op € 974.005, =.
Op dit wetsvoorstel is een voorafgaande toets door het Adviescollege toetsing administratieve lasten (Actal) verricht. Actal heeft in zijn advies van 9 februari 2012 (JtH/FvK/2012/05) een aantal aandachtspunten meegegeven.
Allereerst vraagt Actal hoe de stijging van de administratieve lasten en nalevingskosten van dit wetsvoorstel wordt gecompenseerd. De lastenstijging die uit dit wetsvoorstel voortvloeit zal moeten worden gecompenseerd in het totaal van toe- en afname van lasten waarvoor het ministerie van Veiligheid en Justitie verantwoordelijk is. Op deze plaats kan niet exact worden aangegeven hoe dat gebeurt. Dat zal via de gebruikelijke rapportages plaatsvinden.
Actal vraagt zich vervolgens af of de enkele omstandigheid dat door middel van bewakingscamera's verwerking van persoonsgegevens plaatsvindt, niet leidt tot de conclusie moet leiden dat er sprake is van administratieve lasten, nalevingskosten en regeldruk omdat die lasten nu eenmaal steeds aan de verwerking van persoonsgegevens zijn verbonden. Dit wetsvoorstel brengt geen verandering aan in de voorwaarden die uit de Wbp voortvloeien om al dan niet over te gaan tot het installeren van bewakingscamera's. Inderdaad is het zo dat aan de verwerking van persoonsgegevens door middel van het vervaardigen van camerabeelden steeds enige nalevingskosten zijn verbonden - het toezicht moet immers kenbaar worden gemaakt aan eenieder - maar het wetsvoorstel heeft daarop geen invloed. Regeldruk gaat natuurlijk uit van de voorwaarden die in de gedelegeerde regelgeving nog moeten worden opgenomen. Dat is echter onvermijdelijk, gelet op het gewicht van de betrokken belangen.
Actal verzoekt verder de administratieve lasten gemoeid met de protocolplicht in kaart te brengen. VNO/NCW- MKB Nederland, het Cbp en ICT Office dringen daar ook op aan. Die berekening is hierboven weergegeven.
Actal vraagt tenslotte aandacht voor de noodzaak te kiezen voor het voor de sector minst belastende alternatief. Deze keuze heeft nadrukkelijk de aandacht gehad bij de vormgeving van het wetsvoorstel. Het heeft ertoe geleid dat in een wetsvoorstel een voorziening is getroffen die ertoe moet leiden dat inbreuken met een relatief minder belangrijk effect niet hoeven te worden gemeld.

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 niet dat het Cbp niet meer zal doen dan van de melding kennisnemen en deze gedurende een bepaalde periode zal bewaren. Het Cbp zal deze meldingen moeten beoordelen en een inschatting moeten maken of er

aanleiding is een onderzoek in te stellen. Een onderzoek kan leiden tot de oplegging van handhavingsmaatregelen. Het ligt voor de hand dat de handhaving van artikel 13 Wbp daarbij aandacht krijgt. Ook is het evident dat factoren als de omvang van het datalek, de potentiële gevolgen ervan en de aard van de gegevens daarbij betrokken worden. Het Cbp stelt echter de eigen prioriteiten vast. 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 bestuursorgaan 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 na 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.
De bestuurlijke lasten voor het openbaar ministerie gemoeid met het verlenen van toestemming zijn naar redelijke verwachting overzienbaar. De voorgestelde voorziening betreft immers alleen beelden van camera's die afkomstig zijn van door de verantwoordelijke of beveiligingsdienst zelf vooraf geïnstalleerde bewakingscamera's waarmee openlijk kenbaar toezicht wordt gehouden. Beelden afkomstig van mobiele telefoons of vergelijkbare apparaten vallen buiten de werkingssfeer van dit wetsvoorstel.
De mogelijke aanvullende belasting van de overheid die voortvloeit uit de omstandigheid dat bestuursorganen in hun rol als verantwoordelijke meldingen moeten doen worden niet als bestuurlijke last aangemerkt. Dezelfde lasten rusten in gelijke mate op burgers en bedrijven.

5.3 Positie van rijksoverheid

De Wbp maakt geen onderscheid in verantwoordelijken die tot de publieke sector of de private sector behoren. Op alle verantwoordelijken rusten dezelfde verplichtingen. De rijksoverheid is daarom in beginsel onderworpen aan de meldplicht op grond van het voorgestelde artikel 34a van de Wbp.
Niettemin is er reden afzonderlijk stil te staan bij de positie van de rijksoverheid. Allereerst geldt dat niet de gehele rijksoverheid onderworpen is aan de Wbp. De

gegevenshuishouding van de inlichtingen- en veiligheidsdiensten wordt beheerst door een afzonderlijke wettelijke regeling (Wet op de inlichtingen- en veiligheidsdiensten 2002). De gegevenshuishouding van de politie, de Koninklijke marechaussee en de bijzondere opsporingsdiensten wordt beheerst door de Wet politiegegevens. Voor de Justitiële Informatiedienst van het Ministerie van Veiligheid en Justitie en het openbaar ministerie geldt de Wet justitiële en strafvorderlijke gegevens. De meldplicht geldt dus niet voor deze onderdelen van de rijksoverheid. Het ligt ook niet in de bedoeling voor deze sectoren afzonderlijke meldplichten te ontwikkelen. Meldplichten voor deze sectoren zou direct of indirect leiden tot het geven van inzicht in informatie- en kennisniveaus van deze organisaties. Dat is onverenigbaar met de onderzoeksbelangen die de desbetreffende diensten hebben.
De desbetreffende wetten voorzien overigens in een zeer behoorlijk niveau van gegevensbescherming, juist waar het de rechten van betrokkenen aangaat.
Voor zover de rijksoverheid wel onder het wetsvoorstel valt, verdient het de aandacht dat op rijksniveau een relatief groot aantal grote gegevensverwerkingen worden beheerd. Het ligt voor de hand dat de uitvoering van de meldplicht bij het Rijk op gecoördineerde wijze plaatsvindt. De Rijks-CIO (Chief Information Officer) en de CIO's van de ministeries zullen daartoe uitvoeringsbeleid gaan vaststellen.

5.4 Gevolgen voor de rijksbegroting

Het wetsvoorstel heeft geen gevolgen voor de Rijksbegroting. Hoewel de meldplicht datalekken naar schatting zal leiden tot een aanzienlijk aantal meldingen per jaar, mag verwacht worden dat het overgrote deel van deze meldingen het Cbp geen aanleiding geeft tot een onderzoek of tot handhavingsmaatregelen. Van het Cbp mag worden verwacht dat het een risicogestuurde aanpak hanteert, waarbij prioriteit wordt gelegd bij de aanpak van overtredingen van de Wbp waarbij sprake is van specifieke risico's voor de bescherming van persoonsgegevens. Het Cbp is onafhankelijk en beslist uiteraard zelf welke zaken het oppakt. Na inwerkingtreding van het wetsvoorstel zullen de veranderingen in de werklast voor het Cbp die de meldplicht datalekken met zich meebrengt worden gemonitord. Er kan dan op basis van objectieve cijfers een verantwoorde beslissing worden genomen over eventuele gevolgen voor de formatie en begroting van het Cbp. Indien geconstateerd wordt dat extra financiering nodig is, zal hier voor binnen de begroting van het Ministerie van Veiligheid en Justitie dekking worden gevonden.

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-MKB Nederland, ICT Office, de Nederlandse Vereniging van Banken, het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming, Bits of Freedom en de FNV. Behoudens van de Raad voor de rechtspraak is van al deze instanties een reactie ontvangen. Van het Verbond van Verzekeraars is een spontane reactie ontvangen. Om doelmatigheidsredenen worden deze reacties besproken bij de desbetreffende onderdelen van deze memorie.
Verder is dit wetsvoorstel voorwerp van een internetconsultatie geweest. De internetconsultatie heeft 43 reacties opgeleverd. Die vallen in een aantal categorieën te onderscheiden. In de eerste plaats hebben 9 individuele burgers zelfstandig hun mening over het wetsvoorstel met de overheid gedeeld. Het gaat daarbij om zeer uiteenlopende reacties. Het betreft zowel voorstanders als tegenstanders van beide hoofdonderdelen van het wetsvoorstel. In de tweede plaats hebben 8 burgers gereageerd met een ondersteuning van de zienswijze van Bits of Freedom. In de derde plaats hebben 11 bedrijven, combinaties van bedrijven en adviseurs en advocaten op individuele basis hun

zienswijze aan de overheid uitgebracht. Het betreft hier vrijwel uitsluitend reacties op de voorgestelde meldplicht datalekken. In de vierde plaats hebben 15 bedrijven uit de sector garagebedrijven en benzinestations gereageerd op de voorgestelde verruiming voor het gebruik van camerabeelden. Op www.internetconsultatie.nl is het gebruikelijke verslag van de consultatie geplaatst.

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 is een wijziging van artikel 22, vierde lid, onder c, van de Wbp opgenomen om de 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 nieuw geformuleerde zevende 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.

Artikel I, onderdeel D

Dit onderdeel is toegelicht in paragraaf 4 van het algemeen gedeelte van deze memorie.

Artikel I, onderdeel E

Het Cbp heeft in de afgelopen jaren samenwerkingsrelaties van uiteenlopende aard ontwikkeld met andere toezichthouders op gebieden waar sprake is van aan elkaar grenzende verantwoordelijkheden. Het toezicht op de naleving op de verwerking van persoonsgegevens speelt immers op velerlei terreinen een rol. Ook op terreinen waarop sectorspecifiek toezicht is ingesteld. Op drie specifieke terreinen heeft dit inmiddels geleid tot het vaststellen van samenwerkingsprotocollen. Het eerste betreft het terrein van de telecommunicatie. Het Cbp heeft samenwerkingsprotocollen met de OPTA en met het Agentschap Telecom (AT) van het Ministerie van Economische Zaken, Landbouw en Innovatie. De OPTA draagt (mede) zorg voor het toezicht op de naleving van de hoofdstukken 11 en 13 van de Telecommunicatiewet. In die hoofdstukken vinden belangrijke gedeelten van het gegevensbeschermingsrecht voor de telecommunicatiesector regeling. Het AT draagt specifiek zorg voor het toezicht op de naleving van de bepalingen uit de Telecommunicatiewet met betrekking tot de

dataretentie. Het tweede terrein betreft de zorg. Het Cbp beschikt ook over samenwerkingsprotocollen met de Nederlandse zorgautoriteit (Nza) en met de Inspectie voor de gezondheidszorg (IGZ). De Nza houdt toezicht op de naleving van de Zorgverzekeringswet en heeft uit den hoofde ook bemoeienis met de verwerking van persoonsgegevens door de zorgverzekeraars. De IGZ houdt toezicht op de naleving van een groot aantal wetten op het gebied van de zorg en komt daar in aanraking met de verwerking van persoonsgegevens door zorgaanbieders. Een derde terrein is het gebied van inkomen en sociale zekerheid. De Inspectie SZW houdt toezicht op de uitvoering van de sociale zekerheidswetgeving en komt daar in aanraking met de verwerking van persoonsgegevens door de uitvoeringsinstanties. Het is zonder meer voorstelbaar dat in andere sectoren deze samenwerkingsrelaties ook worden ontwikkeld.
Onverminderd de eigen verantwoordelijkheid van elk van de in aanmerking komende toezichthouders is het voor een efficiënt en effectief toezicht op de naleving van belang dat het Cbp en de andere daarvoor in aanmerking komende toezichthouders elkaar zonodig over en weer toezichtgegevens kunnen verstrekken. In de praktijk blijkt dat zich van tijd tot tijd de noodzaak voordoet dat daarbij ook persoonsgegevens moeten worden verstrekt. Daarvoor is in verband met toepassing van de artikelen 7 en 9 van de Wbp een behoorlijke wettelijke grondslag vereist.
In artikel I, onderdeel E, van het wetsvoorstel is daartoe een voorziening getroffen, mede naar aanleiding van het advies van het Cbp. Het nieuwe artikel 51a van de Wbp is gebaseerd op een van de modellen opgenomen in het bij brief van de Minister van Justitie van 29 oktober 2008 aan de Voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 2008/09, 31 700 VI, nr. 70) gezonden rapport van de Werkgroep herijking toezichtsregelgeving. In verband met de door artikel 28 van de richtlijn gegarandeerde onafhankelijke positie van het Cbp moeten wel enige bijzondere voorzieningen worden getroffen. Er kan geen sprake zijn van een *eenzijdig* op te leggen verplichting - hetzij door de wetgever, hetzij anderszins - tot deze gegevensoverdracht. Dat behoort een zaak van consensus te zijn. Daarom staat in het voorgestelde artikel 51a van de Wbp voorop dat het Cbp bevoegd - dus niet verplicht - is met andere toezichthouders samenwerkingsprotocollen te sluiten. Eerst wanneer aan die voorwaarde is voldaan, kan er sprake zijn van een niet vrijblijvende wederzijdse gegevensverstrekking. Verder ligt het niet voor de hand dat het Cbp dergelijke samenwerkingsprotocollen sluit met bestuursorganen die niet tevens de hoedanigheid hebben van toezichthouder. Dat zou kunnen leiden tot onevenwichtigheden. Het ligt in de bedoeling de gegevensuitwisseling tussen het Cbp en andere instellingen na verloop van tijd - in samenwerking met het Cbp - te bezien om te beoordelen of de samenwerkingsbepaling aan zijn doel beantwoordt.

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 4.1.13 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.

De Tw kent een van de Wbp afwijkende reikwijdtebepaling. Bepalend voor de bevoegdheid van de Cbp is niet de regeling van artikel 4 van de Wbp, die uitgaat van de vestigingsplaats van de verantwoordelijke, maar het feit of de desbetreffende aanbieder van een openbare elektronische communicatiedienst overeenkomstig de Tw is geregistreerd bij de OPTA.

Artikel II, onderdeel G

In paragraaf 4.1.14 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 II, 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

In artikel IV is een samenloopbepaling opgenomen die de verhouding regelt tussen het onderhavige wetsvoorstel en het bij de Eerste Kamer der Staten-Generaal aanhangige voorstel voor een Wet aanpassing bestuursprocesrecht (Kamerstukken 32 450). Dat is noodzakelijk, omdat in artikel III van dit wetsvoorstel een aanpassing moet plaatsvinden van de bijlage bij de Wet bestuursrechtspraak bedrijfsorganisatie, terwijl de inhoud van die bijlage in het voorstel Wet aanpassing bestuursprocesrecht naar de Algemene wet bestuursrecht wordt overgeheveld.

Artikel V

Aangezien de Telecommunicatiewet een ander rechtsbeschermingsregime kent dan de Wbp 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 V bevat daarvoor een voorziening.

Deze memorie is opgesteld onder medeverantwoordelijkheid van de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken, Landbouw en Innovatie.

De Staatssecretaris van Veiligheid en Justitie,