'SOX around the klok'

A.D. Putker-Blees*

40 **Naleving van de Amerikaanse Sarbanes-Oxley Act 2002 (SOX) kan een inbreuk opleveren met de Europese Privacyrichtlijn. Zo verplicht SOX tot invoering van klokkenluidersregelingen met anonieme *hotlines*. De Europese Privacyrichtlijn eist daarentegen dat verwerking van persoonsgegevens onder meer op transparante en zorgvuldige wijze geschiedt. De Artikel 29-werkgroep, het onafhankelijke overlegorgaan van Europese nationale privacytoezichthouders, heeft in een recente 'Opinie' een aantal handreikingen geboden die enige zekerheid trachten te bieden aan bedrijven die zowel aan de SOX als aan de Europese Privacyrichtlijn moeten voldoen. Een inventarisatie.**

Inleiding

'De regel dat men zijn vuile was niet naar buiten moet brengen, lijkt mij, als de was werkelijk vuil is, zeker als algemene rechtsregel uiterst ongezond. De regel wordt ongezonder naar gelang de inwendige toestand van een (...) organisatie voor de buitenwereld meer belang heeft', aldus H. Drion in 1969.[1]

Het naar buiten brengen van de vuile was wordt wel klokkenluiden genoemd. De klokkenluider of *whistleblower* is de werknemer die zonder toestemming en veelal in strijd met zijn geheimhoudingsplicht een misstand in de onderneming waar hij werkzaam is aan de grote klok hangt. Met de onthulling wordt de noodklok geluid om de gemeenschap te waarschuwen voor een specifieke acute of dreigende misstand.[2]

De Amerikaanse Sarbanes-Oxley Act is een reactie op de 'vuile was' bij het Amerikaanse energieconcern Enron en bij WorldCom. Uit onderzoek en juridische procedures bleek dat interne en externe controlemechanismen hadden gefaald. Regelgeving van de SOX gaat niet alleen Amerikaanse genoteerde beursondernemingen en hun bestuurders aan, maar ook beroepsgroepen, zoals juristen en accountants. Europese ondernemingen met een beursnotering in Amerika (*foreign issuer*) dienen zich evenzeer aan voorschriften van de SOX te houden. Daarnaast wordt aangenomen dat er sprake is van een zekere reflexwerking voor Amerikaanse niet-beursgenoteerde ondernemingen.[3]

De SOX verplicht tot een breed scala van maatregelen die eerdergenoemde schandalen moeten voorkomen. Zo moet de SOX tot gevolg hebben dat (financiële) informatie van beursvennootschappen steeds accuraat is en, zo nodig, tijdig openbaar gemaakt wordt.[4]

Section 301(a) van de SOX stelt *audit committees* verplicht om procedures te ontwikkelen voor:

'(...) the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters (...)'

Het gaat derhalve om 'kliklijnen' met een beperkt bereik: uitsluitend het instellen van procedures voor het vertrouwelijk melden van boekhoudkundige of *auditing* misstanden valt hieronder. Bedrijven die niet voldoen aan de voorschriften die de SOX voorschrijft ten aanzien van – bijvoorbeeld – klokkenluidersregelingen lopen het risico van zware sancties door Nasdaq, de New York Stock Exchange of de SEC (Securities and Exchange Commission).

Naar aanleiding van SOX moeten Europese bedrijven met een notering in de Verenigde Staten voldoen aan wettelijke verplichtingen waardoor onder omstandigheden in strijd wordt gehandeld met de voorschriften van de Europese Privacyrichtlijn.[5] Genoemde Privacyrichtlijn beoogt onder meer in alle lidstaten van de Europese Unie dezelfde maatstaven te hanteren ten aanzien van privacybescherming van natuurlijke personen van wie de persoonsgegevens worden verwerkt. Op grond van voornoemde Privacyrichtlijn is in Nederland in 2001 de Wet bescherming persoonsgegevens (WBP) in werking getreden, die onder meer transparant en zorgvuldig gebruik van persoonsgegevens moet waarborgen. Persoonsgegevens zijn alle gegevens betreffende geïdentificeerde of identificeerbare natuurlijke personen.

In de zomer van 2005 heeft de Commission Nationale de l'Informatique et des Libertés (CNIL) – de Franse evenknie van de Nederlandse toezichthouder, het

* Mevr. mr. A.D. Putker-Blees is advocaat bij Stibbe te Amsterdam.

1. H. Drion, 'Het rechterlijk verbod en de vrijheid van meningsuiting', in: *Op de grenzen van komend recht: opstellen aangeboden aan prof. mr. J.H. Beekhuis*, Zwolle: Kluwer 1969, p. 103.
2. *Kamerstukken II* 2002/03, 28 990, nr. 3, p. 1.
3. F.B.J. Grapperhaus, 'Bescherming voor klokkenluidende werknemers: een inventarisatie van het wetsvoorstel en het SER-advies', *Ondernemingsrecht* 2005, 78, p. 232-240.
4. M.J. van Ginneken, 'De Sarbanes-Oxley Act of 2002: het Amerikaanse antwoord op Enron', *Ondernemingsrecht* 2003/3, p. 65-70 en *Ondernemingsrecht* 2004, 54 (p. 150-157).
5. Richtlijn nr. 95/46/EG van de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *PbEG* 1995, L 281.

College bescherming persoonsgegevens – tot tweemaal toe restricties opgelegd ten aanzien van het gebruik van anonieme kliklijnen voor klokkenluiders. Zo moest McDonald's in Frankrijk voldoen aan de Franse privacywetgeving én aan de voorschriften op basis van de SOX. De CNIL meende dat de door McDonald's voorgestelde anonieme kliklijn in strijd was met de Franse privacywetgeving en overwoog: '(...) En outre, la CNIL a estimé que les dispositifs présentés étaient disproportionnés au regard des objectifs poursuivis et des risques de denunciations calomnieuses et de stigmatization des employés objets d'une "alerte éthique". (...)[6]'
Na overleg met de SEC heeft de CNIL op 15 november 2005 op haar website een aantal richtlijnen gegeven voor Franse vennootschappen hoe zij een *Catch-22* situatie kunnen voorkomen. De CNIL vertrouwt erop dat de SEC een positief signaal zal geven aan bedrijven en hen zal geruststellen over de ontstane situatie van onduidelijkheid ten gevolge van tegenstrijdige regelgeving.
In navolging van de CNIL heeft de Artikel 29-werkgroep (hierna: de Werkgroep), het onafhankelijke overleg- en adviesorgaan van Europese nationale privacytoezichthouders, recentelijk een 'Opinie' (hierna: de Opinie) afgegeven, die moet bijdragen aan de rechtzekerheid van bedrijven die zowel aan de Europese als aan de Amerikaanse regelgeving onderworpen zijn.[7] De hoofdlijnen van de Opinie, die niet bindend is voor de lidstaten, maar wel gewicht in de schaal legt, komen overeen met de richtlijnen van de CNIL. De Werkgroep heeft zich in deze Opinie beperkt tot klokkenluidersregelingen op het gebied van accountancy, interne accountantscontrole, *auditing* misstanden, bestrijding van corruptie en financiële fraude.[8]
Het feit dat niet alleen de rechtspositie van de klokkenluider aan de orde is, maar evenzeer de positie van degene die onderwerp is van de beschuldiging, maakt de Opinie extra interessant nu de positie van de beschuldigde vaak onderbelicht blijft in publicaties en regelgeving.[9] De Werkgroep acht het van belang, dat ook degene die in het beklaagdenbankje zit, de bescherming geniet die de Europese Privacyrichtlijn en de implementatiewetgeving hem bieden.
In de Opinie wordt benadrukt dat klokkenluidersregelingen in overeenstemming moeten zijn met voorschriften voor verwerking van persoonsgegevens, zoals beschreven in de Europese Privacyrichtlijn. Het toepassen van de klokkenluidersregeling, waarbij steeds onderzoek zal worden gedaan naar een melding, zal in de meerderheid van de zaken neerkomen op het verwerken van persoonsgegevens waaronder het verzamelen, vastleggen, bewaren, opvragen en doorzenden van gegevens die een geïdentificeerde of identificeerbare natuurlijke persoon betreffen, zoals gedefinieerd in de Europese Privacyrichtlijn.
In het hiernavolgende zullen de uitgangspunten van de Werkgroep ten aanzien van het redigeren en uitvoeren van klokkenluidersregelingen worden toegelicht aan de hand van een aantal bepalingen van de Europese Privacyrichtlijn.

Toelaatbaarheid klokkenluidersregeling

Een rechtsgeldige klokkenluidersregeling moet voldoen aan de vereisten die gesteld worden aan de voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens, zoals genoemd in art. 7 van de Europese Privacyrichtlijn. Een eerste grondslag voor rechtmatigheid kan worden gevonden in de naleving van een nationale wettelijke plicht. Een buitenlandse wettelijke plicht kan hieronder dus niet

6. "Dispositifs d'alerte professionnelle: à quelles conditions sont-ils conformes à la loi informatique et libertés?",15 november 2005, "www.cnil.fr/index.php?id=1890".
7. 'Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime', 'www.europa.eu.int/-comm/justice_home/fsj/privacy/docs/wpdocs/2006/w-p117_en.pdf'. De Werkgroep verwijst overigens naar een uitspraak van de US Court of Appeals (First Circuit) van 5 januari 2006 inhoudende dat de SOX-regelgeving op het gebied van klokkenluiders niet van toepassing is op *foreign citizens* die werkzaam zijn buiten Amerika voor *foreign subsidiairies*. Als deze uitspraak letterlijk wordt genomen zou voor werknemers van Europese dochters van Amerikaanse beursgenoteerde ondernemingen geen expliciete anonieme klokkenluidersregeling behoeven te worden ingevoerd. Het is niet duidelijk wat de implicaties zijn van deze uitspraak nu er geen uitspraak is in het hoogste ressort.
8. Van Essen signaleerde al eerder, dat een deel van de (registratie)regels die de SOX oplegt aan accountantskantoren die auditwerk verrichten voor bedrijven met een rapportageverplichting aan de SEC, niet kunnen worden nageleefd zonder daarmee in strijd te handelen met de WBP: J.M. van Essen, 'Sarbanes-Oxley Act en de WBP', *Privacy & Informatie* 2004, p. 100-106.
9. Zie onder meer E. Verhulp, *Vrijheid van meningsuiting van werknemers en ambtenaren* (diss. Amsterdam), Den Haag: Sdu Uitgevers 1996; A.F. Verdam, 'Bescherming van klokkenluiders: welke regels en procedures (dienen te) gelden?', *ArbeidsRecht* 2001, 3; R.S. van Coevorden, 'De klokkenluider, het geheimhoudingsbeding en art. 7:661 BW', *ArbeidsRecht* 2002, 42, p. 12-21; P. Willems, 'Klokkenluidersbescherming verder ingekleurd, wordt spreken toch goud?', *ArbeidsRecht* 2003, 54 en F.C. van Uden, 'De ondraaglijke stilte van de vrijheid van meningsuiting in het arbeidsrecht', *ArbeidsRecht* 2006, 7.

worden begrepen. De Werkgroep stelt vast dat het niet de bedoeling is dat door buitenlandse wetgeving Europese regelgeving omzeild wordt. De Werkgroep verwijst in een noot expliciet naar de Code Tabaksblat die op basis van art. 2:391 lid 4 BW beursvennootschappen in Nederland verplicht een klokkenluidersregeling in te voeren.[10,11]
Een andere grondslag voor rechtmatige verwerking van persoonsgegevens is dat de regeling noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor verwerking van persoonsgegevens 'verantwoordelijke'[12] of van de derde(n) aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op de bescherming op grond van de Europese Privacyrichtlijn prevaleert. Gelet op het doel van de SOX – melding maken van boekhoudkundige of *auditing* misstanden – kan er sprake zijn van een gerechtvaardigd belang om een klokkenluidersregeling rechtsgeldig te laten zijn, aldus de Werkgroep.

Het eerlijk, rechtmatig en op proportionele wijze verwerken van persoonsgegevens

Uit art. 6 van de richtlijn volgt dat persoonsgegevens eerlijk en rechtmatig moeten worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Persoonsgegevens moeten toereikend, ter zake dienend en niet bovenmatig zijn met het oog op het doel waarvoor zij worden verzameld of waarvoor zij vervolgens zijn verwerkt. Ook moeten alle redelijke maatregelen worden getroffen om verwerkte persoonsgegevens die onnauwkeurig of onvolledig zijn uit te wissen of te corrigeren.
Op grond van art. 6(1)(b) en (c) van de Europese Privacyrichtlijn moeten persoonsgegevens die worden verwerkt worden beperkt tot datgene wat strikt noodzakelijk is om de beschuldiging te verifiëren en mogen de persoonsgegevens niet langer worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor deze worden verzameld of vervolgens worden verwerkt noodzakelijk is. Aan de toepasselijkheid van bovengenoemde criteria van toelaatbaarheid, kwaliteit en proportionaliteit verbindt de Werkgroep de volgende consequenties.

- Met het oog op het beginsel van proportionaliteit moet zorgvuldig afgewogen worden of het aantal personen dat gerechtigd is om onregelmatigheden over een bepaald onderdeel van het bedrijf te melden, beperkt dient te worden. Evenzeer kan het nuttig zijn om het aantal personen dat van onregelmatigheden beschuldigd kan worden te limiteren. De Werkgroep onderkent overigens dat de omstandigheden van het geval steeds doorslaggevend zullen zijn voor het maken van bovengenoemde afwegingen.
- De Werkgroep meent dat bijzondere aandacht op zijn plaats is voor de vraag of het wel wenselijk is dat de klokkenluidersregeling erin voorziet dat er anoniem wordt gemeld in plaats van een melding waarbij sprake is van identificerende gegevens. Natuurlijk moet de klokkenluider wel op vertrouwelijke basis kunnen melden. De Werkgroep meent dat anonimiteit noch voor de klokkenluider noch voor de organisatie een goede oplossing is. Zo zal het onderzoek bemoeilijkt worden als er geen aanvullende vragen kunnen worden gesteld en zal een geruchtenstroom kunnen ontstaan over de identiteit van de klokkenluider. Daarnaast brengt de mogelijkheid van een anonieme melding het risico van een ongegronde melding met zich met als doel het zwart maken van iemand anders uit de organisatie. Ook voor de persoonsverwerking wordt het problematisch als er sprake is van een anonieme melding nu de persoonsgegevens eerlijk en rechtmatig moeten worden verwerkt. De Werkgroep stelt als uitgangspunt dat alleen meldingen die identificeerbaar zijn op grond van de klokkenluidersregelingen moeten worden verwerkt. Het doel van de Werkgroep, het verschaffen van rechtszekerheid, wordt hiermee dus niet (geheel) bereikt. Immers, op basis van de SOX moeten werknemers op vertrouwelijke anonieme basis onregelmatigheden kunnen melden, terwijl de Werkgroep dit op grond van de Europese Privacyrichtlijn afkeurt.

10. De Nederlandse Corporate Governance Code beginselen van behoorlijk ondernemingsbestuur en *best practice*-bepalingen, 9 december 2003, 'www.commissiecorporategovernance.nl'.
11. In deze beschouwing laat ik de in de Stichting van de Arbeid tot stand gekomen gedragscode, het advies van de Commissie Arbeid, Onderneming en Medezeggenschap van de SER aan de Minister van SZW inzake klokkenluiders van 22 december 2004 (SER, Advies van de Commissie Arbeid, Onderneming en Medezeggenschap, *Klokkenluiders*, nr. 04/14, 'www.ser.nl/publicaties/default.asp?desc=b23348'), het initiatiefwetsvoorstel van juli 2003 – dat al weer geruime tijd stilligt (vgl. noot 2), – alsmede de beleidsregels van de Nederlandse Mededingingsautoriteit (Persbericht NMa van 2 december 2005, 'www.nmanet.nl'), ten aanzien van (anonieme) informanten, buiten beschouwing. Voor een overzichtsartikel over de stand van zaken van klokkenluiden in Nederland waarbij ook de regelgeving van klokkenluiden in de VS wordt besproken verwijs ik naar F.C. van Uden, 'Klokkenluiden: tussen zelfregulering en Amerikaanse toestanden', *AA* 55, 2006, p. 33-41.
12. Art. 1 Europese Privacyrichtlijn: '(...) verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.'

Overigens verdient voornoemde kritiek op de Opinie in de Werkgroep meteen enige nuancering, omdat laatstgenoemde ook toegeeft dat zich omstandigheden kunnen voordoen dat de klokkenluider toch op anonieme basis aan de bel trekt. De Werkgroep is *streetwise* genoeg om onder ogen te zien dat veel meldingen nu eenmaal anoniem gebeuren. De Werkgroep meent dat de anonieme melding uitzondering op de regel moet zijn en moet worden ontmoedigd door bedrijven. De klokkenluider moet van de aanvang af of via de klokkenluidersregeling duidelijk worden gemaakt dat zijn identiteit geheim blijft jegens derden, zoals bijvoorbeeld zijn manager en jegens degene die van onregelmatigheden beschuldigd wordt. Als de klokkenluider op grond van deze informatie er toch niet van overtuigd kan worden dat hij voldoende zal worden beschermd en vasthoudt aan een anonieme melding, zal deze toch als zodanig mogen worden geaccepteerd.

- Gegevens die gerelateerd zijn aan een onderzoek mogen niet langer dan twee maanden na afronding van het onderzoek worden bewaard, tenzij disciplinaire maatregelen worden getroffen tegen de melder (valselijke melding) of de persoon over wie werd gemeld (gegronde melding).

Informatieverstrekking moet helder en compleet zijn

Werknemers moeten worden geïnformeerd over het bestaan, het doel en de inhoud van de klokkenluidersregeling. Hierbij moet de werknemer ook worden gewezen op bijvoorbeeld het recht van toegang, van rectificatie en uitwisseling van gegevens die hem of haar betreffen (vgl. art. 12 Europese Privacyrichtlijn). Daarnaast moeten werknemers ervan op de hoogte zijn dat de identiteit van de klokkenluider steeds geheim zal worden gehouden jegens degene die door de klokkenluider beschuldigd wordt.

De rechten van de persoon die beschuldigd wordt van onregelmatigheden

In verband met verplichtingen op grond van de Europese Privacyrichtlijn ten aanzien van de verwerking van persoonsgegevens moet een klokkenluidersregeling ook rekening houden met de rechten van de persoon van wie de persoonsgegevens (bijvoorbeeld in het kader van een onderzoek naar fraude) worden verwerkt zonder afbreuk te doen aan de rechten van de klokkenluider zelf. De Werkgroep benadrukt dat klokkenluidersregelingen ertoe kunnen leiden dat een persoon die onderwerp is van beschuldiging wordt gestigmatiseerd. Onder omstandigheden kan sprake zijn van grove privacyschending, voordat een persoon zich ook maar bewust is van het feit dat hij ergens van wordt beschuldigd, terwijl een formeel onderzoek naar de beschuldiging nog niet eens begonnen is. De Werkgroep is de mening toegedaan dat een correcte toepassing van de Europese Privacyrichtlijn ten aanzien van klokkenluidersregelingen dergelijke risico's van stigmatisering zal verminderen.

Er moet een balans gevonden worden tussen de rechten van degene die beschuldigd wordt en de legitieme behoefte van de werkgever om een onderzoek te doen als melding wordt gemaakt van ernstige onregelmatigheden die de reputatie van de onderneming kunnen bezoedelen. In dat kader is art. 11 van de Europese Privacyrichtlijn van belang, waarbij wordt bepaald dat een betrokkene op de hoogte wordt gesteld wanneer gegevens over hem worden verwerkt die niet bij hemzelf zijn verkregen. Iemand die beschuldigd wordt, zal zo snel mogelijk moeten worden geïnformeerd over bijvoorbeeld de feiten waarvan hij wordt beschuldigd, over degenen die het verslag van de melding zullen ontvangen en over de manier waarop hij zijn recht van inzage, correctie en verzet (art. 14 Europese Privacyrichtlijn) kan uitoefenen. Informatieverstrekking aan de beschuldigde mag uitgesteld worden om te voorkomen dat bijvoorbeeld bewijs wordt vernietigd. De Werkgroep benadrukt dat het uitstel van het verstrekken van informatie aan de beschuldigde terughoudend moet worden gehanteerd en niet als uitgangspunt mag worden genomen.

Beveiliging van de verwerking

De werkgever die een klokkenluidersregeling hanteert, dient overeenkomstig art. 17 van de Europese Privacyrichtlijn zorg te dragen voor passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen vernietiging of bijvoorbeeld niet toegelaten verspreiding. Deze voorzorgsmaatregelen moeten proportioneel zijn en overeenstemmen met de regels die gelden in de verschillende lidstaten. Individuen moeten worden aangespoord om misstanden te melden. Daartoe is het essentieel dat de klokkenluider beschermd wordt door zijn bevindingen vertrouwelijk te behandelen en te voorkomen dat derden zijn identiteit te weten komen. Uitzondering hierop wordt gevormd door het geval dat komt vast te staan dat de klokkenluider opzettelijk misleidende beschuldigingen heeft geuit. In dat geval kan de identiteit van de klokkenluider met het oog op een mogelijke claim van degene die valselijk is beschuldigd worden vrijgegeven, tenzij het nationale recht hiertoe geen ruimte biedt.

Afhandeling van meldingen

De Werkgroep onderkent dat bedrijven wellicht de behoefte hebben om een externe serviceprovider in te schakelen voor de verzameling van persoonsgegevens in het kader van een onderzoek naar mogelijke misstanden. Deze serviceprovider moet op zijn beurt ook weer gebonden worden aan een strikte geheimhouding waarbij wordt voldaan aan de vereisten van art. 16 (vertrouwelijkheid van de verwerking) en 17 (beveiliging van de verwerking) van de Europese Privacyrichtlijn.

Het afhandelen van meldingen dient te geschieden door middel van een specifiek daartoe aangegeven onderdeel van de organisatie met speciaal daartoe opgeleide mensen, die aan een geheimhoudingsplicht worden gebonden. De (werkzaamheden door deze) groep dient gesepareerd te worden van andere afdelingen, zoals de afdeling human resources. De SOX stelt dit soort specifieke eisen overigens niet. De verzamelde en verwerkte persoonsgegevens zullen uitsluitend ter hand worden gesteld aan de mensen die hiertoe op grond van de klokkenluidersregeling zijn aangewezen.

Door de aard en structuur van multinationals kan het zijn dat onderzoeksresultaten in concernverband moeten worden verspreid. In verband met het beginsel van proportionaliteit zal de aard en de ernst van de onregelmatigheid bepalen op welk niveau en in welk land informatie moet worden gedeeld. De Werkgroep neemt als uitgangspunt dat het wenselijk is dat de onderzoeksresultaten lokaal, dat wil zeggen, in één EU-land worden behandeld. Dit verdient de voorkeur boven het delen van de informatie met andere bedrijfsonderdelen in concernverband. De Werkgroep maakt een uitzondering voor de situatie dat er gegevens moeten worden uitgewisseld met een ander onderdeel van de multinational wanneer het onderzoek dit vergt. De Werkgroep geeft aan dat art. 25 van de Europese Privacyrichtlijn (doorgifte van persoonsgegevens naar derdenlanden) en de afwijkingen, zoals beschreven in art. 26 van de Europese Privacyrichtlijn, ook van toepassing zijn. Dit zal zich kunnen voordoen als een bedrijf (een gedeelte van) de uitvoering van de verwerking van persoonsgegevens aan een externe serviceprovider heeft uitbesteed met servers of systemen buiten de EU.

Bedrijven die een klokkenluidersregeling implementeren moeten ook voldoen aan art. 18 en 20 van de richtlijn. Art. 18 verplicht tot aanmelding bij de toezichthoudende autoriteit voordat wordt overgegaan tot een min of meer volledig geautomatiseerde verwerking van gegevens die voor de verwezenlijking van een doeleind bestemd zijn. Art. 20 voorziet in een onderzoek door de toezichthoudende autoriteit naar aanleiding van de aanmelding vóór de aanvang van de verwerking van persoonsgegevens die specifieke risico's met zich brengen voor de rechten en vrijheden van betrokkenen.

Conclusie van de Werkgroep

De Werkgroep onderkent dat een klokkenluidersregeling een goed instrument kan zijn om te voorkomen dat misstanden niet aan de oppervlakte komen. De Werkgroep benadrukt dat de voorschriften van verwerking van persoonsgegevens, zoals neergelegd in de Europese Privacyrichtlijn, volledig moeten worden nageleefd bij het uitvoeren van klokkenluidersregelingen. Voor de klokkenluider en degene die van onregelmatigheden wordt beschuldigd is het van belang dat het fundamenteel recht op bescherming van persoonsgegevens wordt gegarandeerd. De Werkgroep wijst er ook op dat de 'verdachte' recht heeft op informatie, toegang, rectificatie en vernietiging van gegevens. Vanzelfsprekend moet – zoals altijd in het privacyrecht – een belangenafweging plaatsvinden tussen het recht op privacy van degene die verdacht wordt en de belangen van de onderneming om haar reputatie te bewaken en te voldoen aan wet- en regelgeving.

Standpunt CBP

Een multinational heeft in het najaar van 2004 de Nederlandse Minister van Justitie verzocht een vergunning te verlenen als bedoeld in art. 77 lid 2 WBP voor de doorgifte van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt. Het College bescherming persoonsgegevens (CBP) brengt ingevolge art. 77 lid 2 WBP advies uit aan de minister met betrekking tot de vergunningaanvraag.[13]

De multinational had een kliklijn opengesteld waarbij al dan niet anoniem gemeld kon worden. De multinational verwees hiervoor naar de verplichtingen op grond van de SOX. Het CBP beoordeelt of de verwerking van persoonsgegevens rechtmatig geschiedt. Er dient een belangenafweging plaats te vinden tussen het belang in brede zin van het concern bij de kliklijn en de inbreuk op de persoonlijke levenssfeer en de andere rechten en vrijheden van betrokkenen bij de verwerking van zijn gegevens na een melding bij de kliklijn. In verband met de open normen in de WBP wordt deze belangenafweging gemaakt door invulling van de begrippen 'proportionaliteit', 'subsidiariteit', 'ernst van de misstand' en 'de gevolgen voor de betrokkenen'. Daarnaast moet de verwerking van gege-

13. Zie 'www.cbpweb.nl/downloads_uit/z2004-1233.pdf?refer=-true&theme=purple', geraadpleegd op 1 juni 2006.

vens verkregen door het klikken behoorlijk en zorgvuldig zijn en voor een welbepaald uitdrukkelijk en gerechtvaardigd doeleind verzameld worden. De grondslag voor de verwerking moet worden gevonden in art. 8 onder *c* WBP (naleving wettelijke plicht) of onder f WBP (gerechtvaardigd belang). De gevolgen voor deze multinational met een Amerikaanse beursnotering indien zij niet kan voldoen aan de SOX worden door het CBP meegewogen bij een beroep op art. 8f WBP. Het enkele bestaan van een buitenlandse verplichting levert *an sich* nog geen gerechtvaardigd belang op, aldus het CBP. Hoewel de Werkgroep in haar Opinie expliciet melding maakt van de Code Tabaksblat als zijnde invulling van een wettelijke verplichting[14], refereert het CBP aan art. 8f WBP en niet aan art. 8 onder *c*. Anders dan bij de Code Tabaksblat gaat de SOX expliciet uit van de mogelijkheid van het anoniem melden van misstanden. Aangezien een anonieme melding niet wordt geregeld in de Code Tabaksblat, kan deze bezwaarlijk gebruikt worden als basis voor het openstellen van kliklijnen waarin de mogelijkheid van anoniem melden is opgenomen, aldus het CBP naar aanleiding van een vraag van mijn kant.

De huidige praktijk leert dat veel meldingen anoniem gebeuren en dat bedrijven deze niet eenvoudig kunnen negeren, aldus het CBP. Het behandelen van deze anonieme meldingen vereist dat bijzondere waarborgen worden getroffen. Een organisatie mag het gebruik van anonieme meldingen niet aanmoedigen en dient een systeem in het leven te roepen waarbij het uitgangspunt is dat de identiteit van de melder wordt vastgesteld. Het mogelijk maken van confidentiële meldingen waarbij de melder zijn identiteit slechts kenbaar maakt aan een vertrouwenspersoon zelf of op andere wijze confidentieel wordt gehouden, verdient naar het oordeel van het CBP de voorkeur. Het CBP wijdt nog een aantal opmerkingen aan het naleven van de informatieplicht ten aanzien van betrokkene, dat hem betreffende gegevens worden verwerkt. Zo moet duidelijk zijn wie verantwoordelijk is voor de verwerking van persoonsgegevens en welke doeleinden de verwerking heeft.

Het inzagerecht van degene die van onregelmatigheden beschuldigd wordt, mag niet worden gebruikt om achter de identiteit van de melder of andere betrokkenen te komen. Zolang dat met het oog op het veiligstellen van bewijsmateriaal noodzakelijk is, kan het inlichten van degene die geïncrimineerd wordt ex art. 43 WBP tijdelijk worden opgeschort. Deze uitzonderingsmogelijkheid dient, het zal u niet verbazen, restrictief te worden geïnterpreteerd, aldus het CBP.

Het CBP concludeert dat er in beginsel sprake is van een gerechtvaardigd belang ex art. 8 onder f WBP voor deze multinational voor het openstellen van een kliklijn door het moederbedrijf. De multinational dient maatregelen te treffen die het vertrouwelijk melden stimuleren en het anoniem melden afremmen, dan wel voorkomen. Indien aan de voorwaarden wordt voldaan die het CBP in zijn advies vergunningsaanvraag noemt, zal het CBP aan het ministerie van Justitie adviseren de vergunning af te geven.

De Werkgroep heeft bij de totstandkoming van haar Opinie de nodige input gekregen van het CBP; dit blijkt ook wel uit de overwegingen van het CBP die grote overeenkomsten vertonen met de hiervoor besproken Opinie van de Werkgroep.

'Mission accomplished?'

Ik vraag mij af of de Werkgroep er helemaal in is geslaagd om volledige rechtzekerheid te bieden aan bedrijven die niet het gevaar willen lopen in een *Catch-22* situatie te komen omdat zij zowel aan de SOX als aan de Europese Privacyregelgeving moeten voldoen. Zo adviseert de Werkgroep bedrijven om anonieme klachten van werknemers te ontmoedigen, terwijl de SOX hiertoe nu juist verplicht. In het kader van de rechtszekerheid zou het natuurlijk ideaal zijn als de Werkgroep met de SEC tot een vergelijk was gekomen over de wijze waarop aan de SOX kan worden voldaan, zonder in strijd te handelen met de Europese Privacyrichtlijn. Helaas is het (nog) niet zover gekomen. Derhalve is het verstandig voor bedrijven om naast de SOX-regelgeving de aanbevelingen van de Werkgroep ter harte te nemen bij het redigeren resp. uitvoeren van klokkenluidersregelingen. Zoals eerder opgemerkt heeft het privacyrecht tal van open normen die moeten worden ingevuld. Overleg met het CBP kan dan ook nuttig zijn om te bepalen of een regeling 'WBP *proof*' is. Het lijkt mij zinvol voor multinationals die met onderhavige problematiek te maken hebben om met andere multinationals te spreken over collectieve zelfregulering met betrekking tot de omgang met persoonsgegevens op basis van een klokkenluidersregeling, waarna vervolgens op grond van art. 25 WBP door het CBP wordt getoetst of een en ander een juiste uitwerking vormt van de wet. Met een dergelijke verklaring van het CBP hebben werkgevers meer zekerheden ingebouwd en zullen zowel de klokkenluider als degene die beschuldigd wordt wat privacybescherming betreft beter af zijn.

14. Vgl. noot 6.