CBPL

Commissie voor de bescherming van de persoonlijke levenssfeer

Privacy

op de werkvloer: mythe of werkelijkheid?

Adviezen en aanbevelingen van de Privacycommissie rond privacy op de werkvloer

Januari 2015

Voorwoord

Een verantwoording voor de aandacht die de Privacycommissie geeft aan privacy op de werkvloer...

De eerste en belangrijkste reden is uiteraard het feit dat wij allemaal in ons dagelijks leven en arbeid worden geconfronteerd met deze vraag hierover. Wij zijn allemaal wel in de ene of andere rol “betrokken” geweest of geworden met vragen over het toezicht van de werkgever op werknemer. We hebben allemaal wel met het ene of andere petje op (ook als werknemer kan het wel voorkomen dat je de rol van werkgever moet opnemen, als zodanig of als consulent, uitvoerder, ...) dergelijke vragen moeten beantwoorden. Het is dan ook een onderwerp dat enerzijds zeer veel mensen raakt en anderzijds ook een belangrijk maatschappelijk fenomeen betreft. De meest treffende illustratie van dit belang is het feit dat in de loop van de vele jaren talloze vragen werden gesteld aan de Privacycommissie in verband met privacy op de werkvloer. Vele maar ook zeer verscheidene vragen. Vele maar ook zeer concrete vragen. Vele en dikwijls ook “ongemakkelijke” vragen: het is dan ook bijzonder moeilijk antwoorden te geven die algemeen gelden voor zovele zeer verschillende situaties.

Dit laatste is ook een van de redenen waarom de Privacycommissie in haar aanpak vooral heeft gezocht naar een procedurele oplossing: wat is, in het nu van toepassing zijnde recht, de te volgen procedure? Welke algemene antwoorden kunnen gegeven worden? Algemene antwoorden die zo bruikbaar, instrumenteel, mogelijk zijn en methodes aanbieden om de gestelde vragen te kaderen.

Ook vanuit de studie van de rechtspraak en de rechtsleer bleek het zeer moeilijk om algemeen geldende regels te formuleren: niet alleen is er de veelheid van concrete omstandigheden, maar er is ook de vaststelling dat rechtspraak en rechtsleer steeds uitspraak doen over situaties die zich voordien hebben voorgedaan. Rechtspraak is dan ook het werk van de (arbeids-)rechtbanken: concreet en met inachtname van alle mogelijke feiten, omstandigheden en wet- en regelgeving de juiste oplossing voor het reeds ontstane geschil uit te spreken.

Daarom hebben we ons als Privacycommissie vooral gefocust op het preventieve aspect. Daarbij is vooral uitgegaan van de vraag die de werknemer en de werkgever zich stellen over wat er nu kan en moet gedaan worden om een correcte en privacyvriendelijke manier van omgaan met persoonsgegevens en de communicatie ervan (eigen of gebonden aan het werk) te verkrijgen. Met dit thema besteden we aandacht aan hoe dit in de praktijk kan worden gedaan. De ervaring leert dat, alhoewel er geen zaligmakende algemene recepten kunnen uitgeschreven worden, dat een heldere communicatie over wat er kan en mag worden gedaan door zowel de werknemer als de werkgever uiterst belangrijk is. Juridisch is dat vereist (en daarvoor kan het arbeidsreglement dienen), maar ook in de praktijk is er grote behoefte aan “duidelijkheid”.

Wat de Privacycommissie in dit verband kan doen is richtinggevend zijn, maar niet bepalend. Elke organisatie, onderneming, instelling of werkvloer zal uiteindelijk haar privacyregeling en controlemogelijkheden zelf moeten uittekenen.

Als Privacycommissie proberen we de vele vragen over privacy en gegevensbescherming in werksituaties proactief en in hun algemeenheid via onze website te beantwoorden door informatie te bundelen in een themadossier op de website, de veel gestelde vragen en de brochure “Cybersurveillance”. Deze brochure werd reeds in 2012 opgesteld als antwoord op de vele vragen over privacy op de werkvloer.

Vandaag nogmaals aandacht vragen voor deze vraagstellingen is ook aandacht vragen voor mogelijke bijdragen en tussenkomsten, voorstellen en tips van uw kant. Aarzel niet bij te dragen en uw ervaringen of kritiek mee te delen. Wij ervaren immers dat het belangrijk is om inzichten en oplossingen te delen.

Ook al omdat het denken en vooral het afbakenen van de problematiek een hele evolutie achter de rug heeft. Getuige dit citaat: “Ongeacht de methode die wordt gevolgd, moet er een einde komen aan de situatie dat een burger slechts grondrechten heeft buiten de onderneming. De democratisering van het bedrijfsleven is broodnodig. Zoniet moet men niet verwonderd zijn dat werknemers die acht en negen uur per dag, elf maanden per jaar, aan een autoritair regime worden onderworpen, plots geen democraten meer blijken te zijn.”

Eenentwintig jaar geleden schreef Professor arbeidsrecht Patrick Humblet deze zinnen als uitsmijter voor het artikel dat onder de titel “het (grond)recht op privacy: een blinde vlek in het arbeidsrecht” verscheen. 1994: het jaar dat de eerbiediging van het privéleven, en het gezinsleven, werd opgenomen in de Belgische Grondwet (artikel 22), het jaar dat de Privacycommissie haar eerste adviezen over ander dan de haar eigen wet- en regelgeving kon geven (de Privacywet is pas ten volle medio 1995 van kracht geworden). En net nadat het Hof voor de Rechten van de Mens het privacyartikel 8 van het Europees verdrag voor de rechten van de mens buiten de strikte privésfeer had gehaald en verruimd had naar de werkvloer: in het arrest Niemietz t. Duitsland (16 december 1992) overwoog het Hof (onder 29): “La Cour ne juge ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de “vie privée”. Il serait toutefois trop restrictif de la limiter à un “cercle intime” où chacun peut mener sa vie personnelle à sa guise et d’en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l’individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n’y avoir aucune raison de principe de considérer cette manière de comprendre la notion de “vie privée” comme excluant les activités professionnelles ou commerciales: après tout, c’est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d’occasions de resserrer leurs liens avec le monde extérieur”. Maar daarmee was het nog niet meteen duidelijk dat de werkvloer ook onder die bescherming zou vallen: Niemietz was immers een advocaat en het toezicht was er van overheidswege. Maar de fysieke grenzen van de bescherming van de persoonlijke levenssfeer werden toen doorbroken.

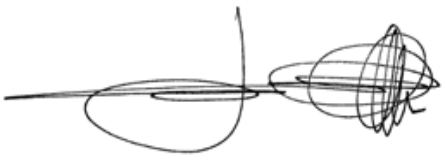
Latere arresten van het Hof hebben deze rechtspraak bevestigd en verder uitgewerkt: Halford t. VK (25 juni 1997) (16 februari 2000) over het afluisteren van de telefoon op de werkvloer (politiekantoor) en Copland t. VK (3 april 2007) over de controle van mail- en surfgedrag van werknemers (kantoor).

In het arbeidsrecht is het wel wachten op de CAO nr. 68 van 16 juni 1998 betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats. Voor het onderwerp dat ons vandaag specifiek aanbelangt, is vooral de CAO nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatiegegevens van groot belang.

Al moet wel vastgesteld worden dat deze typische normen van het collectieve arbeidsrecht niet gemakkelijk doorwerken in het klassieke arbeidsrecht: getuige daarvan de rechtspraak die eigenlijk tot op vandaag op zoek is naar een vaste rechtspraak over deze problematiek.

Er is over die pakweg laatste twintig jaar al veel gebeurd. Niet alleen is het nu gemeengoed geworden dat ook op de werkvloer privacy haar rechten moet kunnen laten gelden. Ook de techniek is danig veranderd, evenals de werkmethode. Alleen al door het gebruik van “own devices”, het internet “of things”, maar ook door sociale netwerken en nieuwe werkvormen, thuiswerk en online, zijn er eigenlijk tal van nieuwe mogelijke probleemsituaties ontstaan. Of is er misschien meer? Misschien komen deze vele vragen rond privacy op de werkvloer voort uit het vervagen van de grenzen tussen de publieke en de private levenssfeer. Misschien is de doorwerking van de bescherming van de persoonlijke levenssfeer naar het “nieuwe werken” ook een teken aan de wand, het verdwijnen van de “offline”, het smelten van de thuishaven?

Het is in tijden van niet aflatende prestatiedwang en steeds grotere blootstelling aan externe druk, en controle in het bijzonder, zeker en vast géén overbodige luxe om voor de rust en de geborgenheid van de persoonlijke levenssfeer te zorgen. Alles van waarde is weerloos leerde ons de dichter. En het beschermen van die persoonlijke levenssfeer en van de communicatie van de persoonlijke gegevens is dan ook een waardevolle opdracht. Ook om goed en degelijk werk te leveren.



Willem Debeuckelaere
Voorzitter Commissie voor de bescherming van de persoonlijke levenssfeer

Stefan Verschuere
Ondervoorzitter Commissie voor de bescherming van de persoonlijke levenssfeer

Privacy op de werkvloer

Adviezen en aanbevelingen van de Privacycommissie

Zowel bij het aangaan van een arbeidsverhouding, gedurende de tewerkstelling zelf, als bij het beëindigen van de arbeidsverhouding worden persoonsgegevens verzameld en verwerkt en duiken dus privacyaspecten op.

Het begint al meteen bij de rekrutering, aangezien bij aanwerving het inwinnen van informatie over de sollicitant centraal staat, onder andere om de geschiktheid van de kandidaat voor de te begeven betrekking te kunnen beoordelen. Met betrekking tot dit luik vindt men onder andere bijdragen terug over het medisch onderzoek, het inwinnen van persoonlijke gegevens over de sollicitant bij derden en over de grenzen van de informatiegaring van de werkgever bij rekrutering.

Eens de betrokkene is aangeworven, zal de werkgever willen weten of hij/zij het afgesproken werk wel correct uitvoert, en zal hij dus tot op zekere hoogte diens doen en laten willen nagaan aan de hand van een aantal controle-instrumenten. Met betrekking tot dit luik vindt men onder andere bijdragen terug over alcohol- en drugcontrole, camerabewaking, het gebruik van badges en naamplaatjes, biometrie, sociale media, geolokalisatie, controle op gebruik van PC (internet, e-mail), telefoon en GSM, het gebruik van klokkenluidersystemen, BYOD (tablet, smartphone), het gebruik van foto's van personeelsleden, eID-kaart verwerkingen m.b.t. medewerkers, toegang tot de professionele elektronische communicatie gevoerd door personeelsleden, de verwerking van evaluatiegegevens over werknemers, callrecording, … Het spreekt voor zich dat de meeste aandacht zal gaan naar privacykwesties die zich kunnen stellen gedurende deze fase van de eigenlijke tewerkstelling.

Tenslotte kan het voorvallen dat de werkgever de betrokkene wil sanctioneren omwille van een bepaalde handeling of gedraging die ongepast, onrechtmatig of onwettig wordt geacht en die blijkt uit een bepaalde verwerking van persoonsgegevens. De werkgever zal deze verwerking, bv. camerabeelden, willen gebruiken om te bewijzen waarom het fout is gelopen met betrokkene ten einde diens ontslag te kunnen motiveren. Met betrekking tot dit luik vindt men onder andere bijdragen terug over de gevolgen van het gebruik van eventueel onrechtmatig verkregen bewijs en andere sancties die een werkgever zouden kunnen ontraden de privacyregels te schenden.

In elk van deze fasen (instroom, doorstroom en uitstroom) moeten uiteraard de fundamentele beginselen die uit het recht op privacy kunnen afgeleid worden (finaliteit, proportionaliteit, transparantie) telkens nageleefd worden. In de bijdragen wordt vaak geschetst hoe de werkgever kan tegemoetkomen aan deze principes bij het verwerken van persoonsgegevens van werknemers.

Bedoeling van deze informatieverspreiding is de werknemers en werkgevers extra alert te maken over het belang van en de noodzaak tot bescherming van de persoonlijke levenssfeer en persoonsgegevens op de werkvloer.

De Privacycommissie heeft rond het thema privacy op de werkvloer veel aandacht besteed en heeft een aantal adviezen en aanbevelingen hieromtrent uitgegeven.

1998

Advies nr. 05/1998 van 30 januari 1998 inzake artikel 314 bis van het Strafwetboek en kwaliteitscontrole in "call centers".

1999

Nihil.

2000

Advies nr. 10/2000 van 3 april 2000 uit eigen beweging betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats.

Advies nr. 32/2000 van 9 november 2000 inzake de overeenstemming van artikel 80 van het koninklijk besluit van 7 augustus 1939 betreffende de evaluatie en de loopbaan van het rijkspersoneel met de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer.

2001

Advies nr. 39/2001 van 8 oktober 2001 uit eigen beweging betreffende het voorstel van wet 2-891/1 van 29 augustus 2001 betreffende het reglementeren van het gebruik van telecommunicatiemiddelen op de werkplaats.

2002

Aanbeveling nr. 01/2002 van 22 augustus 2002 inzake de opname van telefoongesprekken in het kader van bankdiensten.

Advies nr. 08/2002 van 11 februari 2002 uit eigen beweging betreffende de verwerking van persoonsgegevens door particuliere uitzendkantoren. **(Bespreking advies)**

Advies nr. 17/ 2002 van 13 mei 2002 inzake de bekendmaking van de prestatietoelagen die worden toegekend aan bepaalde ambtenaren en de mededeling van de resultaten van individuele loonsonderhandelingen van contractuele personeelsleden aan de representatieve vakorganisaties.

2003

Advies nr. 04/2003 van 10 februari 2003 inzake het ontwerp van koninklijk besluit tot bepaling van de bijzondere aanwervingsvoorwaarden van het statutaire en het contractuele personeel van het Federaal Agentschap voor de Veiligheid van de Voedselketen en tot regeling van de dienst met het oog op het voorkomen van belangenconflicten.

Advies nr. 47/2003 van 18 december 2003 inzake de gedragscode voor de personeelsleden van het Ministerie van de Vlaamse Gemeenschap. **(Bespreking advies)**

2004

Advies nr. 02/2004 van 26 februari 2004 uit eigen beweging betreffende identificatiebadges waarop naam en/of foto van de houder van de badge vermeld staan. **(Bespreking advies)**

Advies nr. 03/2004 van 15 maart 2004 inzake een Ontwerp van besluit van de Vlaamse regering waarbij sommige personeelsleden van de Administratie bevoegd voor Werkgelegenheid van het Ministerie van de Vlaamse Gemeenschap de toelating wordt verleend om persoonsgegevens van de personen uit de kansengroepen te verwerken met het oog op de bevordering van de evenredige participatie op de arbeidsmarkt.

2005

Advies nr. 12/2005 van 7 september 2005 betreffende het wetsvoorstel tot regeling van het toezicht op werknemers door middel van een monitoringsysteem verbonden met het GPS-navigatiesysteem van dienstwagens. **(Bespreking advies)**

Advies nr. 18/2005 van 9 november 2005 met betrekking tot een ontwerpbesluit van de Regering van de Franse Gemeenschap houdende de gedragscode voor gebruikers van informaticasystemen, email en internet binnen de diensten van de Regering van de Franse Gemeenschap, en de instellingen van openbaar nut die onder het Comité van Sector XVII ressorteren. **(Bespreking advies)**

Advies nr. 20/2005 van 30 november 2005 inzake de wetsvoorstellen aangaande het deugdelijk bedrijfsbestuur ("corporate governance") van beursgenoteerde vennootschappen, van overheidsbedrijven en van door de overheid betoelaagde organisaties.

2006

Aanbeveling nr. 01/2006 van 29 november 2006 betreffende de verenigbaarheid van meldsystemen (klokkenluidersystemen) met de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. **(Bespreking aanbeveling)**

Advies nr. 08/2006 van 12 april 2006 betreffende het gebruik van cameratoezicht in een kinderdagverblijf. **(Bespreking advies)**

Advies nr. 07/2006 van 22 maart 2006 betreffende het project "monitoring kansengroepen" in het personeelsbestand van het Ministerie van de Vlaamse Gemeenschap beheerd via het Vlimpers-systeem. **(Bespreking advies)**

Advies nr. 21/2006 van 12 juli 2006 met betrekking tot de deontologische code van de Federale Overheidsdienst Economie, KMO, Middenstand & Energie voor het gebruik van informaticamiddelen en elektronische gegevensverwerking. **(Bespreking advies)**

Advies nr. 22/2006 van 12 juli 2006 met betrekking tot het ontwerp van wet tot wijziging van verschillende bepalingen betreffende het welzijn van de werknemers bij de uitvoering van hun werk waaronder deze betreffende de bescherming tegen geweld, pesterijen en ongewenst seksueel gedrag op het werk.

Advies nr. 34/2006 van 6 september 2006 inzake de adviesaanvraag van het Secretariaat-generaal van het Waals Gewest over het voorstel voor een elektronische bedrijfsgids.

2007

Advies nr. 03/2007 van 7 februari 2007 met betrekking tot de vraag over de verenigbaarheid van de klokkenluiderwerking ingesteld door het Vlaams decreet van 7 mei 2004 met de wetgeving in verband met de privacy. **(Bespreking advies)**

Advies nr. 21/2007 van 23 mei 2007 over de door de Vlaamse Regering goedgekeurde nota met betrekking tot een verhoogde openbaarheid van het beloningsbeleid bij de Vlaamse overheid.
(Bespreking advies)

2008

Advies nr. 05/2008 van 27 februari 2008 betreffende de monitoring van kansengroepen in de schoot van de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding. **(Bespreking advies)**

Advies nr. 21/2008 van 11 juni 2008 betreffende de mogelijkheid voor een werkgever uit de overheidssector om in het raam van een tuchtprocedure gebruik te maken van documenten die door de politie ontdekt werden op de professionele PC van een ambtenaar.
(Bespreking advies)

2009

Nihil.

2010

Nihil.

2011

Advies nr. 32/2011 van 30 november 2011: klacht met betrekking tot de doorgifte van persoonsgegevens door een werkgever aan een provider van mobiele telefonie in het kader van een systeem van gesplitste facturering voor privé –en professioneel gebruik.
(Bespreking advies)

Advies nr. 35/2011 van 21 december 2011 inzake vermelding van de identiteit van een klokkenluider in interne communicatie via e-mail en in de notulen van de vergadering van de raad van bestuur.
(Bespreking advies)

2012

Aanbeveling nr. 07/2012 van 2 mei 2012 uit eigen beweging betreffende de publicatie van foto's van wijkagenten van de lokale politie.
(Bespreking aanbeveling)

Aanbeveling nr. 08/2012 van 2 mei 2012 uit eigen beweging betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer.
(Bespreking aanbeveling)

Advies nr. 16/2012 van 2 mei 2012 over een project om persoonsgegevens in te zamelen uit het personeelsbestand van het Ministerie van het Brussels Hoofdstedelijk Gewest in het kader van het beleid inzake Gelijke kansen en Diversiteit. **(Bespreking advies)**

Advies nr. 36/2012 van 12 december 2012 aangaande een voorontwerp van wet houdende sommige bepalingen van het administratief statuut van het operationeel personeel van de hulpverleningszones en boek 15 van een voorontwerp van koninklijk besluit tot bepaling van het administratief statuut van het operationeel personeel van de hulpverleningszone betreffende het uitvoeren van alcohol- en drugtests.
(Bespreking advies)

2013

Aanbeveling nr. 03/2013 van 24 april 2013 uit eigen beweging over het gebruik van traceertoestellen door politiediensten ten aan zien van hun personeelsleden. **(Bespreking aanbeveling)**

Advies nr. 18/2013 van 5 juni 2013 naar aanleiding van een klacht tegen de installatie van een kwaliteitsgarantieplatform om telefoongesprekken tussen werknemers en potentiële klanten van de werkgever op te nemen. **(Bespreking advies)**

Advies nr. 65/2013 van 18 december 2013 betreffende een voorontwerp van decreet betreffende de opvang van kinderen tot twaalf jaar.
(Bespreking advies)

2014

Nihil.

Bespreking van enkele bovenstaande adviezen en aanbevelingen van de Privacycommissie rond privacy op de werkvloer

Advies nr. 08/2002 van 11 februari 2002
uit eigen beweging betreffende de verwerking van persoonsgegevens door particuliere uitzendkantoren

Dit advies heeft in hoofdzaak betrekking op de activiteiten van de uitzendsector. De opmerkingen van de Privacycommissie kunnen evenwel mutatis mutandis van toepassing zijn op een werkgever die zelf zijn personeel selecteert en rekruteert.

Het is werkgevers algemeen verboden gerechtelijke gegevens met betrekking tot sollicitanten te verzamelen en te bewaren, behalve indien de te begeven betrekking onderworpen is aan regelgeving op grond waarvan een blanco strafregister of een strafregister vrij van bepaalde veroordelingen vereist is (ambtenaar, militair, bewakingsagent, advocaat, ...).

De Privacycommissie trekt tevens de aandacht op het nemen van aantekeningen betreffende fysieke bijzonderheden van de sollicitant tijdens het interview (zwaarlijvigheid, hazelip, ...). De relevantie ervan wordt enkel in een heel klein aantal gevallen voor zeer specifieke betrekkingen aangetoond. De selectie van werknemers gebaseerd op dergelijke criteria zou overigens kunnen worden beschouwd als discriminerend.

De persoonlijkheidstesten of psychotechnische proeven, nodig voor de interpretatie van de resultaten van de specifieke kennis, mogen alleen worden uitgevoerd onder de verantwoordelijkheid van een psycholoog of, indien de sollicitant akkoord gaat, van een persoon die door een psycholoog behoorlijk opgeleid is voor dit soort opdrachten. Een geïmproviseerde analyse van deze testen kan leiden tot onnauwkeurige gegevens en de verwerking van de persoonsgegevens van de kandidaat ongeldig maken (artikel 4, §1, 4°, van de Privacywet).

De Privacycommissie beveelt verder aan enkel vragen te stellen over de gezondheid van de kandidaten wanneer een specifieke betrekking wordt beoogd, en zich in voorkomend geval te beperken tot de objectief noodzakelijke vragen. In de gevallen waarin de uitoefening van de functie geen bijzondere risico's inhoudt, moeten deze vragen achterwege blijven. Zo stellen functies als kantoorbediende, administratief werk, onthaalhostess bij voorbeeld objectief geen enkel bijzonder probleem en zij kunnen derhalve geen vragen over allergieën, astma, gewicht, ... van de betrokken persoon rechtvaardigen.

Gegevens over sollicitanten mogen niet meer worden verwerkt zodra deze personen niet meer geïnteresseerd zijn in het vinden van een betrekking bij betrokken werkgever. Het kan dus nuttig zijn aan de sollicitanten mee te delen dat hun gegevens worden gewist na het verstrijken van een bepaalde termijn, behalve als de kandidaat er anders over beslist (ofwel vraagt hij zijn gegevens sneller te wissen, ofwel verkiest hij daarentegen dat zijn gegevens langer worden bewaard).

Advies nr. 47/2003 van 18 december 2003
inzake de gedragscode voor de personeelsleden van het Ministerie van de Vlaamse Gemeenschap

In dit advies, dat onder andere handelde over "cybermobbing" op de werkvloer, aanvaardde de Privacycommissie dat de verplichtingen en verantwoordelijkheden die in het kader van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk bij de werkgever rusten, een voldoende juridische basis verlenen om in toepassing van artikel 109terE, 1° van de toenmalige wet van 21 maart 1991 (nieuw artikel 125 §1, 1° Wet op elektronische communicatie) als wettelijke uitzondering te gelden op het strafrechtelijk beschermd telecommunicatiegeheim. Meer bepaald aanvaardde de Privacycommissie dat het de werkgever toegelaten is om op basis van de door de ontvanger vrijgegeven inhoud van een e-mailbericht (dat kan worden gekwalificeerd als pesterij, ongewenst seksueel gedrag of als een andere vorm van gewelddadig gedrag) en aan de hand van de loggegevens, het werkstation te traceren van waaruit het e-mailbericht werd verzonden (en dit zonder toestemming van de verzender).

Advies nr. 02/2004 van 26 februari 2004
uit eigen beweging betreffende identificatiebadges waarop naam en/of foto van de houder van de badge vermeld staan.

In dit advies neemt de Privacycommissie standpunt in met betrekking tot het dragen of het moeten kunnen voorleggen van een badge met daarop persoonsgegevens van de houder ervan, hetzij diens foto, hetzij diens naam, hetzij beiden.

Het evenredig karakter van een dergelijke verwerking moet geval per geval beoordeeld worden, aldus de Privacycommissie.

Zo zou de identificatie van de personen die regelmatig in contact staan met het publiek (taxichauffeurs, personen belast met klantenrelaties, loketbedienden van een administratie) als proportioneel kunnen worden beschouwd, maar de identificatie van personen die in diensten werken die voor het publiek gesloten zijn, dan weer niet.

Voor de personen die een gezagsfunctie uitoefenen en gemachtigd zijn om inbreuken vast te stellen (politiefunctionarissen, beëdigde ambtenaren van een publieke vervoersmaatschappij, ...), zou de verplichting om een identificatiebadge te dragen, kunnen beantwoorden aan het proportionaliteitscriterium als dit de burger de mogelijkheid biedt te verifiëren of de persoon die zijn gezag over hem uitoefent daadwerkelijk diegene is die hij beweert te zijn.

Ook het type van instelling en het al dan niet gevoelig karakter van de gegevens die zij verwerkt (bijvoorbeeld de Veiligheid van de Staat of een commerciële onderneming voor huishoudproducten) zijn elementen die in rekening kunnen gebracht worden bij de beoordeling van de proportionaliteit van de verwerking.

Hoe meer persoonsgegevens op de identificatiebadge voorkomen, hoe groter de indringing in de persoonlijke levenssfeer van de betrokken persoon. Het is dus noodzakelijk om zo veel mogelijk te vermijden tegelijkertijd de naam en de foto van de betrokken persoon op de badge te vermelden.

De verantwoordelijke voor de verwerking zal in overleg met de betrokken personen of hun vertegenwoordiger(s) de gegevens die op de identificatiebadge moeten voorkomen evenals de mogelijke alternatieven (naam en/of foto en/of referentienummer, ...) moeten onderzoeken ten opzichte van het te behalen doel. Is het doeleinde de identificatie van de persoon zelf, dan enkel naam, geen foto; is het doeleinde kunnen verifiëren of personen die in de gebouwen van een grote onderneming/administratie rondlopen daartoe gemachtigd zijn dan enkel foto, geen naam. In sommige omstandigheden kan het dragen van een badge waarop zowel foto als naam van de badgehouder voorkomen gerechtvaardigd zijn, bijvoorbeeld ingeval de toegang tot bepaalde lokalen omwille van veiligheidsredenen enkel gereserveerd is voor sommige personen (ambassades, ministerie van landsverdediging, luchthaven, ...).

Behalve in geval het zichtbaar dragen van een badge door een reglementaire tekst wordt opgelegd, moet de verantwoordelijke voor de verwerking in overleg met de betrokken personen of hun vertegenwoordiger(s) afwegen of de badge op een zichtbare manier moet gedragen worden dan wel enkel op verzoek moet worden voorgelegd.

Het finaliteitsbeginsel houdt ten slotte in dat de gegevens niet mogen verwerkt worden op een wijze die onverenigbaar is met het duidelijk bepaald en gerechtvaardigd doel. Zo mag de foto van de werknemer die genomen werd voor de aanmaak van een identificatiebadge niet gebruikt worden voor publicatie op een intranetsite of in een brochure die door de werkgever wordt uitgegeven, zonder dat hem (de werknemer) voor deze andere doeleinden zijn uitdrukkelijk akkoord werd gevraagd en dat op het ogenblik dat de badge werd aangemaakt of op het ogenblik van publicatie op intranet of in een brochure.

Advies nr. 12/2005 van 7 september 2005 betreffende het wetsvoorstel tot regeling van het toezicht op werknemers door middel van een monitoringsysteem verbonden met het GPS-navigatiesysteem van dienstwagens

De kernbepaling van het wetsvoorstel luidde dat “De bewaking door middel van een monitoringsysteem gekoppeld aan een GPS-navigatiesysteem in een dienstwagen die door werknemers wordt gebruikt, is alleen toegestaan na akkoord van de paritaire comités ad hoc, het gemeenschappelijk comité voor alle overheidsdiensten of van de organen bevoegd krachtens het stelsel van de collectieve arbeidsbetrekkingen”.

De Privacycommissie bracht op 7 september 2005 een gunstig advies uit ten aanzien van bedoeld wetsvoorstel:

- mits de instemming van de vakbonden, zoals voorzien in het wetsvoorstel, zou worden verrijkt met de individuele toestemming van de werknemers;
- mits het akkoord tussen de sociale partners uitdrukkelijk zou bepalen met welk doeleinde de bewaking gebeurt.
- dat indien het systeem zou geïnstalleerd worden met de bedoeling de uitvoering van de taken toevertrouwd aan de werknemers te controleren, wat klaarblijkelijk het geval was luidens de Toelichting welke het wetsvoorstel voorafging, dit dan een gerichte controle zou moeten zijn, gerechtvaardigd door aanwijzingen die misbruik door bepaalde werknemers doen vermoeden;
- dat een permanente controle waarbij er middels een lokalisatiesysteem een systematische lezing van de geregistreerde gegevens plaatsvindt, in principe als overmatig zou moeten beschouwd worden;
- dat een regelmatiger controle gerechtvaardigd zou kunnen zijn om het beheer van de verplaatsingen van de professionele voertuigen (verkopers, technici te velde) te optimaliseren waarbij de werknemer naargelang de behoeften van zijn lokalisatie het

systeem gericht kan activeren en desactiveren;

- mits voorzien zou worden in een uitgebreide kennisgeving ten behoeve van de personen wier gegevens verwerkt worden, in het bijzonder wie onderworpen is aan controle, in welke mate er controle is, de aard van de misbruiken die aanleiding kunnen geven tot controle, de duur van de controles, de procedure die zal worden gevolgd na controle;
- mits de werkgever oog heeft voor andere maatregelen die voortvloeien uit de Privacywet en in het bijzonder de aangifte van de verwerking verrichten, de veiligheid en vertrouwelijkheid van de verwerking waarborgen, de rechten van de betrokkenen inzake toegang tot en desgevallend verbetering van hun persoonsgegevens honoreren.

Advies nr. 18/2005 van 9 november 2005
met betrekking tot een ontwerpbesluit van de Regering van de Franse Gemeenschap houdende de gedragscode voor gebruikers van informaticasystemen, email en internet binnen de diensten van de Regering van de Franse Gemeenschap, en de instellingen van openbaar nut die onder het Comité van Sector XVII ressorteren

In dit advies herinnerde de Privacycommissie eraan dat, wat het verzamelen van de communicatiegegevens -en onder meer van eventuele loggings betreft- het beginsel van vertrouwelijkheid van de communicatiegegevens toepasselijk is, dit echter zonder afbreuk te doen aan de noodzakelijke invoering van technische en organisatorische veiligheidsmaatregelen zoals voorzien bij artikel 16 van de Privacywet, bedoeld om de toegang tot het netwerk te beveiligen en op globale wijze de veiligheid van persoonsgegevens te verzekeren.

Tevens wees de Privacycommissie erop dat men zich niet enkel mag laten leiden door de bescherming van de persoonlijke levenssfeer van de gebruikers (dus de personeelsleden) van de informatiesystemen, maar dat ook de privacy van de burgers, wier persoonsgegevens worden verwerkt in die informaticasystemen, moet voor ogen gehouden worden: ook deze dient beschermd te worden. En dit kan in sommige gevallen vereisen dat de verantwoordelijken kunnen nagaan of de gebruikers van het systeem hebben gewerkt in overeenstemming met deze laatste vereiste. De regelgeving dient dan ook een evenwicht na te streven tussen enerzijds de rechtsbescherming van de gebruiker en anderzijds de bescherming van de persoonsgegevens die door de gebruikers worden verwerkt.

De Privacycommissie benadrukte dus eigenlijk dat de eisen inzake e-security op gespannen voet kunnen komen te staan met de privacy van werknemers, niet omdat dit in het loutere belang is van de werkgever, maar omdat de werkgever wettelijk verplicht is ook het privacybelang van andere personeelsleden en derden (klanten, leveranciers, ...) te waarborgen. De werknemer moet, vanuit dit oogpunt bekeken, als het ware een stuk eigen privacy prijsgeven ter bescherming van andermans privacy. De logging van de toegang en de analyse van de logbestanden om ieder eventueel oneigenlijk gebruik achteraf te kunnen traceren is, zo bekeken, dan ook een tweesnijdend zwaard: het laat toe de werknemer te identificeren, hetzij eventueel als slachtoffer van schendingen van privacy door anderen (dus in zijn voordeel), maar ook eventueel als dader van schendingen van andermans privacy (dus in zijn nadeel).

Advies nr. 07/2006 van 22 maart 2006
betreffende het project "monitoring kansengroepen" in het personeelsbestand van het Ministerie van de Vlaamse Gemeenschap beheerd via het Vlimpers-systeem

In dezelfde lijn met advies nr. 05/2008 van 27 februari 2008 betreffende de monitoring van kansengroepen in de schoot van de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding, maar dan betrekking hebbend op verwerkingen van diversiteitsgegevens door de Vlaamse administratie in zijn geheel gaat het advies nr. 07/2006 van 22 maart 2006 betreffende het project "monitoring kansengroepen" in het personeelsbestand van het Ministerie van de Vlaamse Gemeenschap beheerd via het Vlimpers-systeem.

Advies nr. 08/2006 van 12 april 2006
betreffende het gebruik van cameratoezicht in een kinderdagverblijf

Dit advies handelt over het gebruik van cameratoezicht in een kinderdagverblijf. Het betrof een systeem van cameratoezicht (webcams) in een private crèche voor kinderen van 0 tot 3 jaar. Dit initiatief biedt aan de ouders de mogelijkheid om op door de directie van het kinderdagverblijf vastgestelde tijdstippen via het internet het gedrag van hun kind te observeren. Zodoende verkrijgen zij eveneens de mogelijkheid om de andere kinderen, maar ook het personeel van het kinderdagverblijf te observeren, alsook externe partijen (sociale werkers, inspecteurs, animatoren, ...). Het personeel en de ouders worden over dit element van het pedagogisch project van het kinderdag-verblijf ingelicht en worden er zelfs toe gebracht hiermee in te stemmen. Men zal derhalve het kinderdagverblijf in zijn geheel filmen, en alle daar aanwezige personen, gaande van de kinderen tot het personeel, de bezoekers, … . Vervolgens zal men deze beelden, met inbegrip van beelden van onvoorziene omstandigheden (ongevallen, enz.), in "real time" verspreiden via het internet, waar zij voor de ouders te bezichtigen zullen zijn. Evenwel zullen de ouders niet enkel en alleen beelden van

hun eigen kind(eren) kunnen bekijken, doch tevens deze van andere kinderen, de personeelsleden en bezoekers van het kinderdagverblijf. Deze verspreidingsvorm via internet houdt verder het risico in dat de beelden door derden op een al dan niet illegale wijze kunnen worden onderschept.

Tevens kunnen de beelden worden hergebruikt door de ouders of derden voor andere doeleinden dan deze dewelke initieel door het kinderdagverblijf werden beoogd.

Samenvattend betekent het voorgaande dat het verlies van de controle over de videobeelden van de kinderen en het personeel absoluut is, en derhalve kan leiden tot een onrechtmatig hergebruik van de beelden. Voor wat betreft de werknemers van het kinderdagverblijf, stelt zich eveneens de vraag naar de toepassing van de principes van de Privacywet.

Er wordt in dit geval geen toepassing gemaakt van de CAO nr. 68 van 16 juni 1998 betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats omdat de commentaar bij artikel 4 van deze uitdrukkelijk stelt dat de CAO enkel van toepassing is op “camerabewaking” door de werkgever, dus een systeem dat tot doel heeft om de arbeidsplaats te bewaken. In dit geval dient het camerasysteem evenwel om de ouders (“derden” in de relatie werkgever-werknemer) de mogelijkheid te bieden om hun kinderen, en tevens de werknemers van het kinderdagverblijf, te observeren, en dient het derhalve niet voor de bewaking van de arbeidsplaats.

Niettemin kan men wel rekening houden met de daarin opgenomen principes. Zo is het bijvoorbeeld volgens de CAO verboden om de werknemers permanent te filmen, en is camerabewaking in de onderneming maar toegelaten voor het nastreven van specifieke doeleinden. Camerabewaking is derhalve overeenkomstig voormelde CAO slechts in welbepaalde gevallen geoorloofd. In dit geval dient de werkgever er dan ook over te waken dat hij de fundamentele rechten van zijn werknemers inzake de bescherming van hun persoonlijke levenssfeer niet schendt. De werkgever zou zich derhalve voor de rechtvaardiging van de installatie van een webcamsysteem in het kinderdagverblijf, op één van de in artikel 5 Privacywet vermelde elementen moeten beroepen en in dit geval wou hij zich blijkbaar beroepen op de toestemming van de werknemers.

Wat de toestemming betreft, merkt de Privacycommissie op dat dit haar voor de werkgever geen goede basis lijkt om zich op te beroepen. Men kan zich in dit geval namelijk de vraag stellen in hoeverre de personeelsleden werkelijk vrij zijn om hun toestemming te geven of niet, wetende dat dit negatieve consequenties zou kunnen hebben. In elk geval zou er de mogelijkheid moeten worden voorzien voor de werknemers om a posteriori hun toestemming in te trekken, hetgeen in casu evenwel niet vanzelfsprekend lijkt.

In het licht van het voorgaande zou een ander wettelijk alternatief meer geschikt zijn, namelijk artikel 5 f) Privacywet. Echter, indien men de bepalingen van de CAO 68 als referentie neemt, aanvaardt men dat de werkgever voor veiligheidsdoeleinden en slechts in specifieke gevallen de werkgevers kan filmen en dat het belang van de verantwoordelijke voor de verwerking dus overheerst op dat van de werknemers. In het geval van de webcams in kinderdagverblijven, kan het belang van de verantwoordelijke voor de verwerking en het door hem nagestreefde doeleinde, indien niet opgelegd door veiligheidsmotieven, niet rechtvaardigen dat het belang van deze verantwoordelijke voor de verwerking zou overheersen op de fundamentele rechten en vrijheden van de personeelsleden. Derhalve lijkt in dit geval het belang van de gefilmde werknemers van die aard te zijn dat het voorrang verdient op het belang van de verantwoordelijke voor de verwerking.

Samenvattend stelde de Privacycommissie dat het verlies van de controle over de videobeelden van het personeel absoluut is, en derhalve kan leiden tot een onrechtmatig hergebruik van de beelden, waardoor de verwerking als problematisch dient te worden beschouwd in het licht van artikel 4 van de Privacywet.

Advies nr. 21/2006 van 12 juli 2006
met betrekking tot de deontologische code van de Federale Overheidsdienst Economie, KMO, Middenstand & Energie voor het gebruik van informaticamiddelen en elektronische gegevensverwerking

In dit advies wees de Privacycommissie op het bestaan van alle uitzonderingen op het principe van de vertrouwelijkheid van de communicatie, zoals gewaarborgd door artikel 124 van de wet van 13 juni 2005 betreffende de elektronische communicatie en de artikelen 259bis en 314bis van het Strafwetboek. Volgens de wet van 13 juni 2005 betreffende de elektronische communicatie is dat onder meer het geval indien daartoe toestemming werd verkregen van alle andere, direct of indirect betrokken personen (artikel 124 in fine van de wet van 13 juni 2005 betreffende de elektronische communicatie), of wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt of wanneer de bedoelde handelingen worden gesteld met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische communicatiedienst te garanderen (artikel 125 § 1, 1° en 2° van de wet van 13 juni 2005 betreffende de elektronische communicatie).

Dit advies hield dan ook eigenlijk een impliciete wijziging in van advies nr. 10/2000 van 3 april 2000 uit eigen beweging betreffende het

toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats. Volgens dit initieel advies had de werkgever van alle betrokken fysieke personen telkens de toestemming nodig om hem toe te laten kennis te kunnen nemen van een bepaalde communicatie (verkeer, inhoud, ...) ontvangen of verzonden door werknemers via zijn netwerk.

Aanbeveling nr. 01/2006 van 29 november 2006 betreffende de verenigbaarheid van meldsystemen (klokkenluidersystemen) met de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

In tegenstelling tot vormen van verticale controle door het toezichthoudend personeel van de werkgever om diens rechten en belangen te vrijwaren, is er tegenwoordig ook sprake van zogenaamd horizontaal toezicht. In dat verband kan er gewezen worden op de implementatie van klokkenluidersystemen op de werkvloer die toelaten meldingen te registreren van collega's over collega's. Het gebruik van een klokkenluidersregeling impliceert dat er waarborgen moeten voorhanden zijn voor de eerbiediging van het grondrecht op privacy in de zin van artikel 8 Europees Verdrag Rechten Mens en artikel 22 Grondwet, welke ten volle blijven doorwerken in de arbeidsverhouding.

Men kan moeilijk anders beweren dan dat een intern meldsysteem eigenlijk een patronale controle inhoudt op medewerkers via medewerkers.

Dat het controlerecht van de werkgever op de werknemers begrensd wordt door het grondrecht op privacy werd al verschillende keren onderstreept in de rechtspraak van het Europese Hof voor de Rechten van de Mens.

Bovendien kan ook gewezen worden op de visie van de Groep 29 dat "klokkenluidersregelingen een ernstig risico inhouden dat de betrokkene binnen de organisatie waartoe hij of zij behoort, slachtoffer wordt van stigmatisering. Het risico is reëel dat zulks gebeurt nog voordat de betrokkene er weet van heeft dat tegen hem/haar een klacht is ingediend en voordat de gegrondheid van de gerapporteerde feiten is onderzocht. De Groep is van oordeel dat een correcte toepassing van de gegevensbeschermingsregels op klokkenluidersregelingen dat risico kan helpen beperken en zeker niet tot uitholling van het beoogde doel van die regelingen leidt, maar integendeel de werking ervan ten goede zal komen".

Welke zijn nu de voorwaarden waarvan sprake in de aanbeveling van 29 november 2006?

1. Finaliteit

Het gaat over werknemersrapportage m.b.t. thema's die niet via de normale hiërarchische weg kunnen worden gemeld en waarvoor geen specifieke, wettelijk geregelde procedures of organen bestaan. Deze rapportage bevat veelal gegevens van geïdentificeerde of identificeerbare natuurlijke personen (de klokkenluider, de geviseerde persoon, ...).

2. Toelaatbaarheid, eerlijkheid, rechtmatigheid en doelbinding

Toelaatbaarheid

Een meldsysteem kan slechts als legitiem beschouwd worden ingevolge het bestaan van een wettelijke of een reglementaire bepaling die het systeem oplegt in hoofde van de organisatie (artikel 5 c Privacywet) of indien het gebaseerd is op het gerechtvaardigd belang van de organisatie, mits het belang of de fundamentele rechten en vrijheden van de beklaagde niet zwaarder doorwegen (artikel 5 f Privacywet).

Eerlijkheid, rechtmatigheid en doelbinding

Vanuit deze principes vereist de Privacycommissie:

- een duidelijke beschrijving van het toepassingsgebied en het doel van het meldsysteem;
- een duidelijke beschrijving van de procedure voor de indiening en de behandeling van meldingen;
- een duidelijke beschrijving van de gevolgen van terechte en onterechte meldingen;
- een duidelijke aanduiding van de verantwoordelijke van de verwerking waarbij recht van toegang, verbetering en wissing kan worden uitgeoefend;
- van belang is het facultatief karakter om als werknemer over te gaan tot een eventuele melding via het systeem: er kan geen patronale verplichting tot melding worden opgelegd;
- voldoende precisie in meldingen en gemelde informatie;
- in principe is er tevens het verbod op anonieme meldingen (om excessen te vermijden);
- verbod van mededeling van identiteit van melder of elementen die zijn identificatie zouden kunnen mogelijk maken zonder zijn akkoord, tenzij in geval van valse meldingen of lasterlijke aantijgingen;

- noodzaak van behandeling melding door een klachtenbehandelaar:
  - die gehouden is tot een beroepsgeheim, ook t.a.v. leidinggevenden, andere personeelsleden en vakorganisaties;
  - die optreedt met voldoende onafhankelijkheid;
  - die optreedt met waarborgen op afwezigheid van onverenigbaarheden;
  - die optreedt met duidelijke aansprakelijkheid;
- de behandeling van melding door de klachtenbehandelaar stopt bij bewuste schending van vertrouwelijkheid van de melding door de melder;
- geen bijkomende arbeidsrechtelijke bescherming gewoon t.g.v. indiening van de melding omwille van mogelijke nefaste effecten – gemeen recht geldt;
- wel bescherming van de melder en de beklaagde tegen fouten van klachtenbehandelaar.

3. Proportionaliteit

Een beperking van het toepassingsgebied van het meldsysteem is eveneens noodzakelijk:

- complementair karakter: enkel meldingen m.b.t. thema's die niet via de normale hiërarchische weg kunnen worden gemeld en waarvoor geen specifieke, wettelijk geregelde procedures of organen bestaan;
- enkel meldingen m.b.t. voldoende zwaarwegende feiten (inbreuken op regelgeving die van toepassing is op de betrokken organisatie of geformaliseerde interne bedrijfsregels op financieel, boekhoudkundig of strafrechtelijk vlak);
- enkel meldingen van personen die tot de organisatie behoren;
- enkel meldingen tegen personen die tot de organisatie behoren en die actief zijn in de domeinen waarop het meldsysteem van toepassing is.

De klachtenbehandelaar moet zorgen dat persoonsgegevens:

- relevant en niet-overmatig zijn voor de behandeling van de melding;
- toereikend zijn voor de behandeling van de melding;
- beperkt blijven tot aanduidingen van feiten, en in principe geen waardeoordelen bevatten;
- die onbewezen feiten uitmaken, uitdrukkelijk als dusdanig worden aangemerkt;
- niet langer worden bewaard dan voor de behandeling van de melding, inclusief de eventuele gerechtelijke of tuchtprocedures tegen de beklaagde of tegen de melder in geval van valse meldingen of lasterlijke aantijgingen.

4. Juistheid en nauwkeurigheid

De klachtenbehandelaar heeft de verantwoordelijkheid om, desgevallend met hulp van voldoende onafhankelijke interne of externe instanties (om bepaalde verificaties te laten verrichten), erover te waken dat de persoonsgegevens voor de behandeling van de meldingen juist en nauwkeurig zijn.

5. Transparantie

Collectief niveau

De organisatie die een meldsysteem wil installeren, moet daarover zijn personeel inlichten, en de wetgeving inzake collectief arbeidsrecht eerbiedigen (door desgevallend informatie te verstrekken aan de ondernemingsraad, het comité voor preventie en bescherming op het werk of, de vakbondsafvaardiging of de onderhandelings- of overlegcomités).

Individueel niveau

Alle medewerkers van de organisatie dienen op de hoogte te worden gesteld van:

- Het toepassingsgebied en het doel van het meldsysteem:
  - de procedure voor de indiening en de behandeling van meldingen;
  - de gevolgen van terechte en onterechte meldingen;
  - de wijze waarop en de instantie waarbij de rechten op toegang, verbetering en wissing kunnen worden uitgeoefend;
  - de derden aan wie persoonsgegevens m.b.t. de melder en de beklaagde kunnen worden doorgegeven in het kader van de behandeling van de melding, bijvoorbeeld de dienst interne audit als de klachtenbehandelaar bepaalde zaken moet laten verifiëren;
  - de melder moet worden gewezen op verplichting tot vertrouwelijkheid bij het indienen en tijdens de behandeling van de melding;
  - de beklaagde moet door de klachtenbehandelaar zo spoedig mogelijk worden ingelicht over het bestaan van een melding en over de hem ten laste gelegde feiten om zijn verdediging te kunnen laten gelden;
  - de inlichting van de beklaagde kan worden uitgesteld in uitzonderlijke omstandigheden (vb. risico op vernietiging van bewijsmateriaal).

6. Veiligheid

- Waarborgen dat persoonsgegevens verwerkt voor de behandeling van meldingen niet voor andere doeleinden worden verwerkt;

- Waarborgen van de integriteit, de authenticiteit, de beschikbaarheid en de vertrouwelijkheid van de persoonsgegevens;
- Waarborgen dat persoonsgegevens niet onrechtmatig kunnen vernietigd worden tijdens de behandeling van de melding;
- Waarborgen van de auditeerbaarheid van de verwerking van de persoonsgegevens;
- Waarborgen van de anonimiteit van de melder en eventuele tussenkomende partijen.

7. Rechten van de betrokkenen (melder, beklaagde, eventuele derden)

- Recht op toegang tot en verbetering van onjuiste persoonsgegevens die hen betreffen, zonder recht op toegang tot de persoonsgegevens over derden, tenzij met hun akkoord;
- Recht op wissing van persoonsgegevens die hen betreffen en onvolledig of niet ter zake dienend zijn, waarvan de verwerking verboden is, of die na verloop van de behandeling van de melding worden bewaard;
- Recht van de beklaagde op toegang tot persoonsgegevens over derden, in het geval van, wat na onderzoek, een valse melding of lasterlijke aantijging (klokkenluider) of een valse getuigenis is gebleken (derde);
- Recht van de klokkenluider om te weten wat met zijn melding wordt gedaan en welke gevolg eraan wordt gegeven;
- Recht van de klokkenluider op toegang tot persoonsgegevens over derden, wanneer na onderzoek is gebleken dat de klokkenluider werd geraakt door de informatie aangebracht door een kwaadwillige beklaagde (die bijvoorbeeld stelde dat de melder zelf betrokken was in de wanpraktijken die hij meldde) of door derden ter kwader trouw (valse getuigen).

Indien rekening wordt gehouden met alle bovenstaande principes in de aanbeveling verdragen dergelijke klokkenluidersystemen zich met de Privacywet.

Advies nr. 03/2007 van 7 februari 2007
met betrekking tot de vraag over de verenigbaarheid van de klokkenluiderwerking ingesteld door het Vlaams decreet van 7 mei 2004 met de wetgeving in verband met de privacy

In dit advies wordt het belang van een beperkt inhoudelijk toepassingsgebied van een klokkenluidersregeling onderstreept.

In dat advies gaat de Privacycommissie onder meer na of het door het Vlaams decreet van 7 mei 2004 opgerichte klokkenluidersysteem verenigbaar is met de Privacywet. Zij is van oordeel dat het toepassingsgebied van het Vlaams meldsysteem te ruim en dus buitensporig is, gelet op het risico op het onrechtmatig en onevenredig aan de kaak stellen van de professionele of zelfs de persoonlijke integriteit van de personeelsleden van de administratieve overheden van de Vlaamse Gemeenschap en het Vlaams Gewest.

De Privacycommissie meent dat klokkenluidersystemen hun toepassingsgebied voor de meldingen moet beperken tot de domeinen van de boekhouding, de interne boekhoudkundige controles, de audit (organisationeel, boekhoudkundig, ...), de strijd tegen de corruptie en de bank- en financiële inbreuken, of bijzonder zwaarwichtige feiten, feiten die gepreciseerd worden in een statuut of in een «gedragscode». Teneinde een betere bescherming van de privacy van de personeelsleden van de administratieve overheden van de Vlaamse Gemeenschap en het Vlaams Gewest te verzekeren, dringt de Privacycommissie erop aan dat de aard van de «onregelmatigheden» die kunnen worden aangeklaagd via het meldsysteem worden ingeperkt tot feiten die laakbaar zijn ingevolge specifieke wetten of tot bijzonder zwaarwichtige feiten die een ernstige negatieve impact kunnen hebben op het functioneren of de reputatie van de administratie. Om het even welk “misbruik” of “nalatigheid” (zie artikelen 3 § 2 en 12bis van het voormelde decreet) kan niet het voorwerp vormen van een dergelijke procedure.

Advies nr. 21/2007 van 23 mei 2007
over de door de Vlaamse Regering goedgekeurde nota met betrekking tot een verhoogde openbaarheid van het beloningsbeleid bij de Vlaamse overheid

Dit advies heeft betrekking op de ambitie van de Vlaamse overheid een verhoogde openbaarheid te geven aan haar beloningsbeleid.

Publieke verantwoording en openbaarheid zijn voor een overheid van cruciaal belang wil ze het vertrouwen van de burger blijven genieten. De Vlaamse belastingsbetaler is immers als het ware de aandeelhouder van de Vlaamse overheid. Een verhoogde openbaarheid schept de nodige legitimiteit voor de overheid om eenzijdige maatregelen te nemen en een beleid te voeren dat directe of indirecte gevolgen heeft voor elke burger, onderneming of maatschappelijke organisatie.

Daarbij moet wel een goed evenwicht gevonden worden tussen de bescherming van de persoonlijke levenssfeer enerzijds en de vraag naar transparantie anderzijds.

Er is geen bezwaar tegen het toegankelijk communiceren op het internet van het algemene beloningsbeleid van de Vlaamse over-

heid zodat de Vlaamse ambtenaren hun loopbaan beter kunnen plannen en externen duidelijkheid krijgen over wat ze financieel mogen verwachten van een betrekking bij de Vlaamse overheid op de verschillende niveaus. Eén en ander kan geduid worden als actieve openbaarheid van bestuur.

Per statutaire functie van het top en middenkaderniveau zal die informatie thans geconcentreerd op de website van de Vlaamse overheid worden geplaatst : salarisband, maar ook andere direct financiële voordelen, zoals mandaattoelage, vakantiegeld, eindejaarstoelage, aangevuld met summiere informatie over het statuut, de functieklasse, het dienstverband. De Privacycommissie heeft uiteraard geen bezwaar. Er wordt immers geen specifieke salarisinformatie over individuele, met naam vernoemde personen openbaar gemaakt. Overigens, voor statutaire personeelsleden worden de salarisschalen, vergoedingen en toelagen, veelal verspreid over meerdere bronnen en teksten, nu reeds gepubliceerd in het Belgisch Staatsblad.

De Privacycommissie heeft verder geen bezwaar dat er op de internetsite een berekeningsprogramma wordt opgenomen waarbij een burger op anonieme wijze een functie en anciënniteit aanduidt en als resultaat informatie krijgt over de beloningsvoorwaarden voor een bepaalde functie bij een bepaalde anciënniteit.

Bovendien zou jaarlijks voor iedereen op organisatieniveau binnen de Vlaamse overheid een naamlijst ter beschikking worden gesteld van de personen binnen de Vlaamse overheid aan wie een toelage werd toegekend. De lijst vermeldt, naast de namen, de grootte van de toelage uitgedrukt in een percentage van het bruto jaarsalaris. Per individu worden dus geen individuele bedragen vrijgegeven.

Personeelsleden die verdere informatie wensen over de motivering van de toekenning van een toelage aan een personeelslid binnen hun entiteit hebben inzage in het document op basis waarvan de toelage werd toegekend. Personeelsleden die verdere informatie wensen over de motivering van de toekenning van een toelage aan een personeelslid buiten hun entiteit dienen hun persoonlijk belang aan te tonen.

Het onderscheid tussen de inzage in de namenlijst enerzijds en de inzage in het document op basis waarvan een toelage werd toegekend anderzijds, beschouwt de Privacycommissie als een uiting van proportionaliteit, en is, op zich, een goede zaak.

Gelet op de finaliteit van de interne bekendmaking van deze persoonsgegevens - om redenen van interne billijkheid en objectivering wordt ernaar gestreefd het vertrouwen van de personeelsleden te krijgen, te behouden en te versterken door meer openheid te creëren rond het toekennen van toelagen - verzet de Privacycommissie zich niet tegen een jaarlijkse bekendmaking van de bedoelde naamlijst onder de personeelsleden van eenzelfde entiteit. Wel heeft de Privacycommissie bedenkingen bij het feit dat personeelsleden van entiteit x inzage zouden kunnen krijgen in de namenlijst van entiteit y. De interne bekendmaking van de namenlijst zou dus beperkt moeten worden per entiteit.

De Privacycommissie stelt ook voor om de documenten op basis waarvan een toelage wordt toegekend in principe niet toegankelijk te maken voor andere personeelsleden. Indien desondanks zou worden vastgehouden aan een zekere inzage in de bewuste documenten door andere personeelsleden, is de Privacycommissie van oordeel dat door het betrokken personeelslid minstens steeds een concreet belang hiertoe moet worden aangetoond ongeacht hij al dan niet werkzaam is binnen dezelfde entiteit als de persoon aan wie een toelage werd toegekend.

Advies nr. 05/2008 van 27 februari 2008 betreffende de monitoring van kansengroepen in de schoot van de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding

In het kader van haar beleid inzake gelijke kansen en diversiteit wil de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (hierna VDAB), een zicht krijgen op de aanwezigheid van de kansengroepen “personen van allochtone afkomst” en “personen met een arbeidshandicap” via de vrijwillige registratie in haar personeelsbestand.

De opname van gegevens met betrekking tot diversiteit (in casu de registratie als allochtoon en/of mindervalide) in het personeelssysteem is toegelaten door een decreet van 8 mei 2002 houdende evenredige participatie op de arbeidsmarkt, het besluit van de Vlaamse regering van 24 december 2004 houdende maatregelen ter bevordering en ondersteuning van het gelijkekansen- en diversiteitsbeleid in de Vlaamse administratie en het personeelsstatuut van de Vlaamse overheid.

De antwoorden op vragen naar afkomst en/of arbeidshandicap geschieden louter op voluntaristische basis, zoals trouwens vereist door artikel 4 van voornoemd besluit.

De vrijwillige verwerking van bedoelde gegevens past in het kader van duidelijke, in de regelgeving omschreven doeleinden (evenredige participatie, bevordering en ondersteuning van het gelijkekansen- en diversiteitsbeleid) en de te verwerken gegevens (gegevens m.b.t. diversiteit), zijn, uitgaande van die doeleinden, toereikend, terzake dienend en niet overmatig.

De betrokkene wordt ingelicht van de beoogde verwerking op het ogenblik dat hij er zal aan onderworpen worden en van zijn rechten en plichten ter zake.

De toegang tot de gegevens m.b.t. diversiteit en de verwerkingsmogelijkheden van de verschillende gebruikers (HRM-dienst en Cel Emancipatiezaken van VDAB) werden gedimensioneerd en beperkt tot wat kan doorgaan als hun rechtmatige behoefte op informatie. Een gradueel striktere toegangsregeling houdt daardoor gelijke tred met de toename van de risico's voor de betrokkene.

Het personeelslid heeft toegang tot de eigen gegevens omtrent afkomst en arbeidshandicap. Dit slaat zowel op het invoeren, het raadplegen of het afvoeren van de eigen gegevens in 'mijn personeelsdossier'.

Men kan besluiten tot het voorhanden zijn van een op vrijwilligheid gebaseerde en voldoende transparante, beveiligde en proportionele bevraging naar gegevens m.b.t. diversiteit voor gerechtvaardigde finaliteiten die overigens mede gebaseerd zijn op decretale rechten en plichten.

Aanbevelingen

Het bijhouden van de historiek van de wijzigingen aangebracht door de betrokkene zelf of op diens vraag in het personeelssysteem, doorkruist het inkeerrecht bij het geven (of het weigeren) van een eerdere toestemming tot de verwerking. De door de betrokkene veranderde gegevens in deze of gene zin mogen dus niet blijvend worden gearchiveerd in het systeem.

De periode voor de implementatie van het zelfregistratiesysteem mag niet samenvallen met een evaluatieperiode, aangezien de indruk kan ontstaan dat personeelsleden die tot de betrokken kansengroepen behoren onder druk worden gezet hun gegevens aan te melden.

Het onverkort opvragen van de nationaliteit van de (groot)ouder(s) van het personeelslid is overmatig. Het verdient aanbeveling gebruik te maken van ruimere klassen om de eerbiediging van het proportionaliteitsbeginsel te waarborgen. VDAB dient uiteindelijk enkel te weten of een personeelslid al dan niet onder de definitie van "persoon van allochtone afkomst" valt. Het beoogde gelijkekansen- en diversiteitsbeleid van VDAB is immers niet gericht op specifieke nationaliteiten.

Er mag geen monitoring worden opgezet van personeelsleden die enkel op basis van de eigen nationaliteit tot de kansengroep "personen van allochtone afkomst" behoren, indien zij zich niet als dusdanig en vrijwillig hebben laten registreren voor de monitoringdoeleinden als bedoeld in dit project. Het kan dus zijn dat iemand theoretisch wel behoort tot de kansengroep op basis van de eigen nationaliteit, maar niet in die hoedanigheid wil behandeld en benaderd worden door VDAB (positieve actie, voorbehouden betrekkingen, ...).

De Privacycommissie wijst nog op het na te leven artikel 25 van het KB van 13 februari 2001, gelet op gevoelig karakter van de op te vragen gegevens. Dit impliceert het opmaken van een lijst met de personen die de gegevens zullen raadplegen, met hun bevoegdheden. Deze lijst moet ter beschikking van de Privacycommissie worden gehouden en deze personen moeten wettelijk, contractueel of statutair tot vertrouwelijkheid verplicht zijn. Tevens moet in de kennisgeving (artikel 9 Privacywet) of in de aangifte (artikel 17 Privacywet) vermeld worden welke wettelijke basis VDAB heeft om deze gegevens in de verwerking op te nemen.

Het verdient aanbeveling, als overkoepelende veiligheidsmaatregel (artikel 16 Privacywet), het gehele project onder toezicht te plaatsen van een informatieveiligheidsconsulent, belast met onder meer de taken van een aangestelde voor de gegevensbescherming (artikel 17bis Privacywet).

VDAB dient er over te waken dat de toetsing op betrouwbaarheid en representativiteit van het systeem (nagaan hoeveel mensen die tot de kansengroepen behoren hun gegevens effectief opgeven in het systeem) niet wordt gerealiseerd aan de hand van persoonsgegevens, bv. door een bevraging bij de HRM-dienst of het verkregen aantal klopt met hun subjectieve waarneming. Het gaat dan enkel over een subjectieve appreciatie van een cijfer en niet over het verzamelen en verwerken van persoonsgegevens.

Advies nr. 21/2008 van 11 juni 2008
betreffende de mogelijkheid voor een werkgever uit de overheidssector om in het raam van een tuchtprocedure gebruik te maken van documenten die door de politie ontdekt werden op de professionele PC van een ambtenaar

Dit advies wil een antwoord bieden op de vraag of de administratie elementen en documenten die door de politie werden aangetroffen op de professionele PC van een ambtenaar mag gebruiken in het raam van een tuchtprocedure en hoe de administratie toegang kan krijgen tot deze elementen en documenten: via een directe toegang in de hoedanigheid van werkgever, dan wel via een aan het parket gerichte vraag.

Wat de aanwending betreft van strafrechtelijke onderzoeksgegevens in een tuchtonderzoek, stelt de Privacycommissie dat het eigen is aan elk onderzoek, ook strafrechtelijk of disciplinair, dat gewerkt wordt met persoonsgegevens die oorspronkelijk met het oog op een andere finaliteit werden ingezameld, maar waarvan de verdere verwerking in het kader van een dergelijk onderzoek wel kan worden verwacht.

Volgens de Privacycommissie is de administratie gerechtigd persoonsgegevens te verwerken van één van haar ambtenaren die voortkomen uit een opsporing- of gerechtelijk onderzoek. Vermits zij instaat voor het tuchtrecht over deze ambtenaar, komt het haar als tuchtrechtelijke overheid dan ook toe deze gegevens te verwerken.
Politie en justitie zijn ertoe gerechtigd de door hen gekende gegevens door te geven aan de betrokken administratie of deze daartoe toegang te geven in de mate dat dit gebeurt in het kader van het wettelijk en reglementair omschreven tuchtrecht.

Algemeen wordt aangenomen dat het Openbaar Ministerie een bijzondere adviserende en informerende taak, met juridische draagwijdte, heeft ten overstaan van de bestuurlijke overheden. Voor een normaal voorzichtig ambtenaar zou het overigens duidelijk moeten zijn en tot zijn normale verwachtingen moeten behoren dat gegevens die vanuit een strafrechtelijk onderzoek werden vernomen door de justitiële autoriteiten kunnen worden overgemaakt aan de disciplinaire autoriteiten. Het spreekt overigens voor zich dat strafrechtelijke informatie mag gebruikt worden in het raam van een tuchtprocedure, eens het strafrechtelijk vonnis werd uitgesproken.

Wat de toegang betreft door de administratie, in haar hoedanigheid van werkgever, tot de PC, hetzij rechtstreeks, hetzij via een vraag aan het parket, meent de Privacycommissie dat indien het gelet op de omstandigheden van de feiten mogelijk is, een toegang door een onafhankelijk orgaan zoals het parket meer waarborgen biedt op de naleving van de rechten van de werknemers dan een rechtstreekse toegang door de werkgever. De elementen zullen inderdaad verzameld worden door een onafhankelijk orgaan dat bovendien beschikt over de noodzakelijke juridische instrumenten om de bewijskracht en de integriteit van de verzamelde elementen te verzekeren.

Een rechtstreekse toegang door de werkgever zou evenwel niet strijdig zijn met de privacy indien de controle punctueel is en gerechtvaardigd door aanwijzingen die een ongerechtvaardigd gebruik van de werkinstrumenten laten vermoeden. De controle zou in voorkomend geval overigens op een dusdanige wijze moeten uitgevoerd worden dat zij beperkt blijft tot de elementen die strikt noodzakelijk zijn voor de tuchtprocedure.

Advies nr. 32/2011 van 30 november 2011

klacht met betrekking tot de doorgifte van persoonsgegevens door een werkgever aan een provider van mobiele telefonie in het kader van een systeem van gesplitste facturering voor privé -en professioneel gebruik

De klager ontving van zijn werkgever een GSM die hij voor professionele en voor private doeleinden kan gebruiken. Voor privécommunicaties dient hij telkens vooraf een specifieke code in te tikken, zodat deze rechtstreeks aan hemzelf kunnen gefactureerd worden. De professionele gesprekken worden evident aan de werkgever gefactureerd. Men noemt deze methode “split-billing”.

De klager werd door zijn werkgever gevraagd om enerzijds een overeenkomst inzake het privégebruik van mobiele telefonie te tekenen, waarin onder andere stond dat “de gebruiker er zich mee akkoord verklaart om zijn adresgegevens aan de provider door te geven”, en om anderzijds een contract te onderschrijven met de provider. Hoewel hij geen van beide contracten ondertekende – omdat hij stelde dat hij de GSM nooit voor privé-doeleinden zou gebruiken – ontving hij opeens een factuur van de provider. Het betrof weliswaar een nulfactuur, maar hieruit leidde de klager af dat zijn gegevens door zijn werkgever toch aan de provider waren doorgegeven.

Hij diende daarop klacht in bij de Privacycommissie.

De Privacycommissie merkt op dat de gangbare praktijk bij het ter beschikking stellen van een GSM door een werkgever erin bestaat om de werknemer drie opties aan te bieden.

Naast het systeem van “split billing”, is het mogelijk om de werknemer te laten kiezen voor de betaling van een forfaitair bedrag, dan wel voor de ondertekening van een document waarin de werknemer op erewoord verklaart dat het GSM-gebruik strikt beperkt blijft tot professionele communicatie en dus elk privé-gebruik ervan wordt uitgesloten.

Wanneer de werknemer opteert voor het forfaitaire bedrag en de werkgever bij nazicht van de kosten vaststelt dat deze substantieel hoger zijn, dan kan de werknemer daarop worden aangesproken om de reden hiervoor te achterhalen en kan de werkgever indien nodig maatregelen treffen.

Hetzelfde geldt wanneer zou blijken dat de werknemer die een verklaring op erewoord deed, de professionele GSM toch voor privédoeleinden zou aanwenden. In deze situaties zullen alle uitgevoerde communicaties verondersteld worden om een professioneel karakter te hebben en de werkgever is dus gerechtigd om deze te controleren (telefoonnummers, tijdstippen, enz.) zonder dat er specifieke maatregelen worden genomen om privé-informatie te beschermen.

Het “split-billing” systeem heeft als belangrijke troef dat de werkgever de factuur voor het privégebruik van de GSM niet te zien krijgt, wat evident positief is voor de bescherming van het privéleven van de

werknemer. Maar deze methode impliceert noodzakelijkerwijze dat de persoonsgegevens van de werknemer ter beschikking gesteld worden van de telefoonprovider.

In deze zaak had de werkgever dus enkel het systeem van split-billing aan de klager voorgesteld. Deze laatste werd quasi verplicht om een overeenkomst te ondertekenen waarin hij instemt met het "split-billing"-systeem.

Toelaatbaarheid

Hoewel de Privacycommissie oordeelt dat het systeem van gesplitste facturering een belangrijk voordeel heeft op het vlak van privacybescherming, meent zij dat de werknemer geheel vrij moet kunnen beslissen of hij al dan niet gebruik wenst te maken van een professionele GSM voor privé-doeleinden. Het patronaal gezag van de werkgever reikt niet zo ver dat laatstgenoemde dit zou kunnen opdringen.

Daarnaast stelt de Privacycommissie ook vast dat de werkgever de gegevens van de klager aan de provider doorgaf, ook al had de klager de "split-billing" overeenkomst – waarin onder andere stond dat er een doorgifte van gegevens zou zijn – niet ondertekend. De doorgifte kan dus niet gesteund worden op artikel 5, a) (toestemming) of 5, b) (overeenkomst) Privacywet aangezien de klager steeds geweigerd heeft om de overeenkomst te ondertekenen.

Gezien de werkgever enkel de "split-billing"-overeenkomst voorlegde aan de klager (zonder hem de twee ander opties voor te stellen) en laatstgenoemde bovendien weigerde het contract te tekenen – meent de Privacycommissie dat de doorgifte van gegevens aan de provider ook niet kan gesteund worden op artikel 5, f), Privacywet (het gerechtvaardigd prioritair belang van de verantwoordelijke voor de verwerking). Had de werkgever immers de twee andere opties ook aangeboden (verklaring op eer of betaling van een forfaitair bedrag), dan was het immers niet noodzakelijk geweest om de gegevens van de klager aan de provider door te geven.

Transparantie

Zelfs al mocht artikel 5, f), Privacywet, toch kunnen weerhouden worden, dan nog kan niet worden ontkend dat de werkgever voorafgaand aan de doorgifte de betrokkene ervan op de hoogte had moeten brengen (cf. artikel 9 Privacywet) dat zijn gegevens – ondanks zijn weigering – alsnog zouden worden doorgegeven aan de provider. Aangezien dit niet gebeurde, handelde de werkgever in elk geval in strijd met het principe dat persoonsgegevens op een eerlijke en een transparante wijze moeten verwerkt worden.

Aanbevelingen

De Privacycommissie beveelt ten aanzien van de werkgever aan om op het vlak van het gebruik van de GSM de eerder aangehaalde opties te voorzien in het arbeidsreglement en de werknemers dienen per optie geïnformeerd te worden omtrent de consequenties die deze opties met zich meebrengen op het vlak van de verwerking van hun persoonsgegevens en omtrent de sanctie ingeval de gemaakte afspraken niet worden nageleefd.

Advies nr. 35/2011 van 21 december 2011 inzake vermelding van de identiteit van een klokkenluider in interne communicatie via e-mail en in de notulen van de vergadering van de raad van bestuur

Dit advies heeft betrekking op een Vlaamse ambtenaar die een klacht had ingediend tegen zijn werkgever (overheidsinstantie), wegens een vermeende schending van de Privacywet. De betrokkene laakte dat zijn identiteit als klokkenluider binnen de administratie ruchtbaar gemaakt werd door communicatie via e-mail enerzijds en door een naamsvermelding in de notulen van de raad van bestuur anderzijds, aangezien die door alle personeelsleden geraadpleegd kunnen worden en in het kader van de openbaarheid van bestuur ook door derden opgevraagd kunnen worden.

In dit advies wordt dan ook gehamerd op de discretie bij elke vorm van communicatie die de identiteit van een klokkenluider kan onthullen, minstens gedurende de looptijd van het onderzoek door de Vlaamse ombudsman.

Tevens beveelt de Privacycommissie ten aanzien van de werkgever aan om de volgende acties te ondernemen:

- de werkgever stelt interne richtlijnen op die discretie voorschrijven bij elke vorm van communicatie die de identiteit van een klokkenluider kan onthullen, minstens gedurende de looptijd van het onderzoek door de Vlaamse ombudsman en eventueel gedurende de volledige looptijd van de bescherming. Bijvoorbeeld zou in e-mailverkeer in beginsel enkel gesproken mogen worden over "de klokkenluider";
- de werkgever stelt interne richtlijnen op wat betreft de rapportering aan de raad van bestuur inzake klokkenluiders, net als voor de wijze van verspreiding van de notulen naderhand;
- de werkgever vervangt de notulen van de raad van bestuur van juni 2008 die intern beschikbaar zijn voor alle personeelsleden door een geanonimiseerde versie. Een integrale versie van de notulen kan uiteraard in het archief bewaard worden, voor zover de toegang hiertoe beperkt blijft tot bevoegden. Hetzelfde geldt voor notulen van andere vergaderingen van de raad van bestuur die de identiteit van de klokkenluider zouden vermelden, minstens voor vergaderingen gehouden gedurende de looptijd van het onderzoek door de Vlaamse ombudsman en eventueel

gedurende de volledige looptijd van de bescherming;
- indien externen op grond van de openbaarheid van bestuur een kopie van de notulen van juni 2008 opvragen, stelt de werkgever ook de geanonimiseerde versie ter beschikking (gedeeltelijke openbaarmaking ter vrijwaring van de persoonlijke levenssfeer). Hetzelfde geldt voor notulen van andere vergaderingen van de raad van bestuur van de werkgever die de identiteit van de klokkenluider vermelden.

Aanbeveling nr. 07/2012 van 2 mei 2012
uit eigen beweging betreffende de publicatie van foto's van wijkagenten van de lokale politie

Deze aanbeveling strekt ertoe de toepassing van de Privacywet te onderzoeken binnen het kader van de publicatie van foto's van wijkagenten in een brochure of op de website van een politiezone.

Ze heeft dus betrekking op de verspreiding van foto's door of in naam van een hiërarchische overheid met de bedoeling de betrokken agenten kenbaar te maken bij de burgers uit de wijk waar hij werkzaam is. De publicatie van afbeeldingen veronderstelt de verzameling, de vastlegging en bewaring van gegevens met behulp van geautomatiseerde middelen. De afbeelding van een geïdentificeerde of identificeerbare persoon op een foto is een persoonsgegeven. Wanneer het gaat om foto's waarop wijkagenten staan afgebeeld in de uitoefening van hun functie via een officiële publicatie vanwege hun hiërarchische overheid, is de Privacywet volledig van toepassing.

Bij de publicatie van foto's van wijkagenten is de korpsoverste de hiërarchische overste, die in principe de verantwoordelijk is voor de verwerking.

Het doeleinde dat wordt nagestreefd, nl. de foto van de wijkagent publiceren zodat de politiefunctionaris gekend is, die belast werd met buurttaken die een rechtstreeks contact vergen met de wijkbewoners, is welbepaald, uitdrukkelijk omschreven en gerechtvaardigd. Hij is inderdaad belast met operationele activiteiten, zoals verzoeningspogingen en informatieverstrekking van de eerst lijn. Het is niet omdat de wijkagent voor de meeste wijkbewoners een gekend figuur is, dat de gehele bevolking van het gebied waar hij werkzaam is, zijn fysionomie kent. Dit is onder meer het geval voor de nieuwe inwoners of als het een dicht bevolkte buurt betreft. Voor dergelijke verwerking is de toestemming van de wijkagent niet relevant. De Privacycommissie meent dat de betrokken personen weliswaar inspraak moeten hebben bij de uitvoering van deze verwerking maar dat die verwerking evenwel niet enkel op grond van de toestemming kan of moet geregeld worden.

De publicatie van de foto van de betrokken agenten is in feite noodzakelijk en gerechtvaardigd voor de goede werking van de diensten van een lokale politiezone. Die publicatie draagt bij aan de vooropgestelde transparantie in het organisatorische beleid van de politiediensten en ligt in de lijn van de wettelijke definitie inzake wijkwerking.

De Privacycommissie acht het niettemin aangewezen dat een recht op verzet wordt erkend en toegekend vooraleer de foto gepubliceerd wordt. De wijkagenten moeten hiervoor een redelijke termijn krijgen. Overeenkomstig artikel 12, §1, 2de lid Privacywet, moeten zwaarwegende en gerechtvaardigde redenen die verband houden met zijn bijzondere situatie de basis vormen voor de uitoefening van dit recht. Het verzet steunt op feitelijke gegevens, bijvoorbeeld de criminaliteitscijfers van de betrokken politiezone of de risico's die de betrokken agent blijkbaar loopt, etc. Indien de verantwoordelijke voor de verwerking niet ingaat op dit recht op verzet, moet hij zijn beslissing motiveren.

Krachtens artikel 4, §1, 3° van de Privacywet moet de verantwoordelijke voor de verwerking waken over de proportionaliteit van de verwerking, dit wil zeggen dat de gegevens toereikend, ter zake dienend en niet overmatig mogen zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt.

Er moet in het licht van dit proportionaliteitsbeginsel vooral rekening worden gehouden met de verspreidingswijze van de bedoelde foto's. De Privacycommissie schuift twee communicatiemethodes naar voor: communicatie via een papieren folder en communicatie op de website van de lokale overheid.

De papieren publicatie komt tegemoet aan de vereiste van gepaste gebruikte middelen voor de welbepaalde doeleinden gelet op het feit en aangezien:

- de publicatie gebeurt op initiatief van de hiërarchische overheid van de betrokken agenten;
- de publicatie uitsluitend verspreid zal worden op het grondgebied waar de agent werkzaam is.

Wat de publicatie van de foto van wijkagenten op het internet betreft, mag de toegang uitgaande van de nagestreefde doeleinden slechts plaatsvinden via het officiële portaal van de politiezone waartoe de wijkagent behoort.

Om te kunnen garanderen dat de bedoelde verwerking niet afwijkt van het nagestreefde doeleinde, raadt de Privacycommissie aan om technische middelen in te schakelen.

Aangezien een website in principe universeel toegankelijk is, is het moeilijk, zo niet onmogelijk om na te gaan of het finaliteitbeginsel geëerbiedigd wordt. Het is met de moderne technieken mogelijk om de gegevens voor andere doeleinden te gebruiken dan de doeleinden waarvoor de gegevens oorspronkelijk werden ingezameld. Uitgaande van de nagestreefde doeleinden is een dergelijke verspreiding van de beeltenis van de wijkagenten overmatig. Om hieraan te verhelpen moet de verantwoordelijke voor de verwerking technische maatregelen inschakelen om de blootstelling van de informatie te beperken en moet hij ervoor zorgen dat het doelpubliek voor wie de informatie bedoeld is werd bepaald en dat derden die informatie niet kunnen misbruiken voor boos opzet (bijv. wraakacties, etc.).

Er moet worden verhinderd dat de zoekmachines refereren naar de afbeelding van de betrokken agent, met name als die gelinkt is aan zijn naam. Als blijkt dat er toch een dergelijke indexatie bestaat, moet de korpsoverste verzoeken deze referenties weg te halen. Ook moeten alle technische middelen aangewend worden zodat het onmogelijk is een kopie van de afbeelding op te slaan in een bestand of af te drukken op een printer.

Het is de bedoeling dat aan de gebruiker, die zijn wijkagent wil kennen via de website van de lokale overheid, wordt gevraagd om de wijk waar hij woont te vermelden door bijvoorbeeld zijn straatnaam te selecteren. Zodra een wijkagent een andere aanstelling krijgt of een gerechtvaardigd verzet tegen de hem betreffende verwerking aantekent, moet de verwerking worden stopgezet en moet zijn foto worden verwijderd.

Aanbeveling nr. 08/2012 van 2 mei 2012 uit eigen beweging betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer

De Privacycommissie bracht op 2 mei 2012 een aanbeveling uit inzake patronale controle op het gebruik door werknemers van elektronische communicatie-instrumenten op de werkvloer, en meer bepaald e-mail en internet. Deze aanbeveling werd vooraf onderworpen aan een publieke consultatie en de respons hierop heeft mee bijgedragen tot het eindresultaat.

Enkele stellingnames in de aanbeveling:

- Patronale toegang tot elektronische communicatie(gegevens) is niet enkel een kwestie van controle op werknemers of zij geen misbruik maken van het e-mailsysteem van de werkgever, maar belangt eveneens de organisatie en beheer van de professionele informatiestroom binnen de onderneming of het openbaar bestuur aan;
- Aangezien er verschillende wetsbepalingen zijn waaraan de toelaatbaarheid van de patronale kennisname van elektronische communicatie(gegevens) moet worden getoetst, benadrukt de Privacycommissie enerzijds dat, voor een juist begrip, het onontbeerlijk is deze bepalingen in hun geheel (en dus gezamenlijk) te lezen en zet zij zich anderzijds af tegen een interpretatie van dit wettelijke arsenaal als zou patronale toegang eigenlijk onmogelijk/onwettig zijn;
- Ondanks zijn verplichting de persoonlijke levenssfeer van werknemers te eerbiedigen, moet de goede werking van de onderneming/het openbaar bestuur immers verzekerd kunnen blijven. Zo niet zou dit kunnen leiden tot meer verdoken en onbeheerste monitoringpraktijken, wat uiteindelijk de bescherming van de persoonlijke levenssfeer van werknemers helemaal niet dient;
- Het werkgeversgezag, uitgedrukt in verschillende wettelijke bepalingen, waaronder de Arbeidsovereenkomstenwet van 3 juli 1978, vormt de juridische toelating om als werkgever kennis te kunnen nemen van bepaalde communicatie ontvangen of verzonden door werknemers via het netwerk van de onderneming of het openbaar bestuur;
- De eventuele toestemming van de werknemer met betrekking tot een dergelijke controle of het gebrek eraan voegt niets toe of doet niets af aan het principiële recht van de werkgever om het gebruik door werknemers van de ter beschikking gestelde online communicatiemiddelen te controleren, kennis te nemen van hun online communicatiegegevens en deze persoonsgegevens te verwerken, aangezien die verwerkingen noodzakelijk zijn met het oog op de uitvoering van de specifieke verplichtingen en rechten van de werkgever met betrekking tot het arbeidsrecht;
- Op basis van de Privacywet kan patronale toegang alleen worden toegestaan indien is voldaan aan de 3 belangrijkste beginselen, waarvan de naleving essentieel wordt geacht voor de bescherming van de persoonlijke levenssfeer van werknemers: een toegang voor legitieme finaliteiten (een doelgebonden toegang), conform het evenredigheidsbeginsel (een proportionele toegang) en met medeweten van de betrokken gebruikers (een voorzienbare toegang);
- Afhankelijk van het doel (beheer of controle), slaat de patronale toegang hetzij op communicatiegegevens die betrekking hebben op een werknemer (en zijn correspondent) en tot stand komen in uitvoering van zijn arbeid, hetzij op communicatiegegevens die betrekking hebben op een werknemer (en zijn correspondent) en tot stand komen in de beleving van de persoonlijke levenssfeer van betrokkene op de arbeidsplek;
- De aard van de gegevens is cruciaal voor het bepalen van de omvang van de toegang door de werkgever (toegang tot de communicaties zelf of enkel tot de elektronische communicatiegegevens);
- Gegevens die tot stand komen in uitvoering van de arbeid van een werknemer zijn op zich relevant voor de werkgever (bv. professionele mail), ook ten aanzien van hun inhoud. Enkel

toegang tot de inhoud van een zakelijk elektronisch bericht kan ervoor zorgen dat de werkgever zijn doel realiseert (bv. de verderzetting van de zakelijke correspondentie verzekeren in afwezigheid van een werknemer);

- Gegevens die tot stand komen in de beleving van de persoonlijke levenssfeer van betrokken werknemer op de arbeidsplek (bv. privémail), worden daarentegen slechts relevant voor de werkgever, in eerste instantie wat hun bestaan betreft, in de mate dat zij de goede uitvoering van de arbeid in het gedrang brengen (met name in geval van strafbare, onrechtmatige of ongeoorloofde privémail);
- Vraag daarom aan werknemers om dubbel gebruik (zowel professioneel als privé) van het professionele e-mailsysteem te vermijden zodat de communicaties verondersteld worden een professioneel karakter te hebben en de werkgever dus gerechtigd is om deze te controleren.

Bij gemengd gebruik daarentegen zullen hoe dan ook specifieke maatregelen moeten worden genomen om privé-informatie bijkomend te beschermen en dit type informatie dus in eerste instantie zoveel mogelijk te ontzien bij controle, bijvoorbeeld door de werknemer te vragen de berichten die hij stuurt en ontvangt te classificeren. Zonder de medewerking van de gebruiker is het anders erg moeilijk het onderscheid correct te maken. In dat geval mogen als “privé” geclassificeerde e-mails pas worden geïndividualiseerd (toegeschreven worden aan een specifieke werknemer) -al dan niet via een directe procedure, zie het getrapt systeem in CAO nr. 81- hetzij wanneer globale controle anomalieën of een concrete aanwijzing van misbruik aan het licht heeft gebracht, hetzij wanneer los van de globale controle een concreet vermoeden van misbruik aan het licht komt (bijvoorbeeld wanneer een derde een concreet feit meldt of door een toevallige ontdekking).

De aanbeveling geeft ook enkele nuttige “watch-outs” en suggesties mee om inbreuken op de bescherming van de persoonlijke levenssfeer van werknemers te minimaliseren in het kader van patronale toegang tot hun elektronische communicatie(gegevens):

- voorzie inspraak en consultatie van de werknemersvertegenwoordiging met betrekking tot het toegangsbeleid;
- leg het toegangsbeleid tot elektronische communicatie(gegevens) van werknemers vast in een geschreven document;
- stel de werknemers in kennis van de na te leven regels en voorwaarden voor de toegang;
- neem preventiemaatregelen om misbruik van internet en e-mail door werknemers te vermijden;
- controleer, indien preventie niet zou volstaan, op misbruik enkel aan de hand van het bestaan van bepaald e-mailverkeer of surfgedrag en dit volgens het stappenplan waarin CAO nr. 81 voorziet;
- controleer, indien het bestaan van bepaald e-mailverkeer of surfgedrag niet volstaat om misbruik vast te stellen, slechts uitzonderlijk door kennisname van de inhoud van communicatie waaraan de werknemer heeft deelgenomen;
- beperk de intrusiemogelijkheden van een werkgever met betrekking tot informatie opgeslagen in de eindapparatuur van een afwezige eindgebruiker;
- zorg ervoor dat de persoon die met een toegang wordt belast een andere persoon is dan degene die daartoe de opdracht geeft;
- zorg ervoor dat de persoon die met een toegang wordt belast tewerk gaat op basis van zo nauwkeurig mogelijke instructies van de opdrachtgever en dat hij zich in zijn zoektocht beperkt tot wat hem werd gevraagd;
- zorg ervoor dat de toegang gebeurt op basis van relevante criteria die toelaten een maximaal aantal gegevens uit de raadpleging te weren;
- zorg ervoor dat de persoonsgegevens die door toegang rechtmatig worden opgezocht en ingezameld blijven verder genieten van hun oorspronkelijke bescherming;
- neem geen belangrijke beslissing tegen een werknemer louter op basis van informatie die ingezameld werd naar aanleiding van een verwerking van zijn persoonsgegevens;
- biedt de betrokkene, alvorens enige beslissing jegens hem te nemen, de mogelijkheid zijn standpunt naar voor te brengen, onder andere wat de juistheid en relevantie van de ingezamelde persoonsgegevens betreft;
- hou alle intrusieverrichtingen in de informatica-instrumenten bij om controle op de naleving van het finaliteitsbeginsel en het proportionaliteitsbeginsel mogelijk te maken;
- stel een aangestelde voor de gegevensbescherming aan die toezicht- en controleverrichtingen en toegangen tot de informaticatools kan beoordelen op hun noodzakelijk en rechtmatig karakter;
- geef een opleiding “gegevensbescherming” die bijdraagt tot de responsabilisering van de werknemers en tot goede praktijken in hoofde van het toezichthoudend personeel.

Deze aanbeveling werd op beknopte wijze samengevat in een informatiebrochure “cybersurveillance” genaamd. Deze brochure bevat eveneens een aantal veelgestelde vragen rond deze materie. De brochure is zowel elektronisch downloadbaar als op papier beschikbaar (op aanvraag).

Advies nr. 16/2012 van 2 mei 2012

over een project om persoonsgegevens in te zamelen uit het personeelsbestand van het Ministerie van het Brussels Hoofdstedelijk Gewest in het kader van het beleid inzake Gelijke kansen en Diversiteit

Het Ministerie van het Brussels Hoofdstedelijk Gewest wenst in het kader van zijn beleid inzake Gelijke kansen en Diversiteit, gegevens in te zamelen die betrekking hebben op de afkomst van zijn personeelsleden.

Het Ministerie wil het aantal personeelsleden kennen dat beantwoordt aan de omschrijving van een persoon van vreemde origine, zoals dat werd vastgesteld door de Regering van het Brussels Hoofdstedelijk Gewest, namelijk: "Persoon met de nationaliteit van een land buiten de Europese Unie (samenstelling van de EU op 1 januari 1995 (EU – 15 lidstaten)) of de persoon waarvan tenminste een ouder of twee grootouders de nationaliteit hebben van een land buitende de Europese Unie".

De gegevens zullen in het personeelsbestand van het Brussels Hoofdstedelijk Gewest worden bijgevoegd zodat het Ministerie die informatie kan koppelen aan andere gegevens die in dit bestand beschikbaar zijn om fijnere statistieken te kunnen opmaken (wat een verwerking van niet anonieme persoonsgegevens rechtvaardigt).

De Privacycommissie is van mening dat het hier geen verwerking betreft van gevoelige gegevens omdat het al dan niet afkomstig zijn uit een van de 15 lidstaten niet toelaat de raciale of etnische afkomst van de betrokkenen te achterhalen.

De verwerking vindt zijn wettelijke grond in de opdracht van openbaar belang waarmee het Ministerie werd belast (krachtens een Ordonnantie, niettegenstaande deze niet precies genoeg is om te kunnen dienen als wettelijke basis van de verwerking) en de toestemming van de betrokkenen.

De Privacycommissie stelt zich vragen over het toereikend karakter van de ingewonnen gegevens omdat de omschrijving zijn basis vindt in het begrip van de Europe Unie (Gemeenschap) in 1995 (15 lidstaten) en niet op de EU zoals die vandaag bestaat. Omdat dit niet werd verantwoord, is de Privacycommissie van oordeel dat het gegeven niet toereikend en niet ter zake dienend is.

De Privacycommissie verlangt dat de gegevens slechts worden bewaard zolang de betrokken persoon een functie uitoefent bij het Brussels Hoofdstedelijk Gewest. De personen worden ingelicht maar de Privacycommissie wenst die informatie verder aan te vullen zoals voorgesteld.

De Privacycommissie verzoekt om na te denken over de personen die toegang zullen hebben tot die informatie. Het project is nu soms onsamenhangend op dit punt.

Het Ministerie verzamelt momenteel het gegeven betreffende de afkomst van de personen niet. Het betreft dus een bijkomende informatie maar wordt gerechtvaardigd door zijn opdracht van openbaar belang in het kader van de uitvoering van het diversiteitsplan.

Het Ministerie eerbiedigt het proportionaliteitsbeginsel van de gegevens omdat het geen precieze gegevens vraagt over de afkomst van de personen (exacte nationaliteit van de werknemers en hun grootouder of ouders). Een gelijkaardig project bij het Ministerie van de Vlaamse Gemeenschap wilde dergelijke gegevens inwinnen en de Privacycommissie had dit bekritiseerd (advies nr. 07/2006 van 22 maart 2006 betreffende het project "monitoring kansengroepen" in het personeelsbestand van het Ministerie van de Vlaamse Gemeenschap beheerd via het Vlimpers-systeem).

De Privacycommissie aanvaardde dat in het kader van dit project van het Ministerie van de Vlaamse Gemeenschap de gegevens in het personeelsbestand werd geïntegreerd.

In het geval het project gevoelige gegevens zou willen toevoegen (bv. m.b.t. gehandicapte personen – wat werd bepaald in de nota die de Brusselse Regering goedkeurde) (en zoals dit het geval was bij het Ministerie van de Vlaamse Gemeenschap), is er een meer uitdrukkelijk omschreven, wettelijke basis noodzakelijk (ordonnantie, besluit), dan de basis die vandaag bestaat (cfr. deze met betrekking tot het Ministerie van de Vlaamse Gemeenschap dat door de Privacycommissie werd goedgekeurd: daar was inderdaad sprake van een specifiek decreet van 8 mei 2002 houdende evenredige participatie op de arbeidsmarkt en een specifiek besluit van de Vlaamse regering van 24 december 2004 houdende maatregelen ter bevordering en ondersteuning van het gelijkekansen- en diversiteitsbeleid in de Vlaamse administratie).

In deze materie heeft de Privacycommissie voordien gelijklopende standpunten ingenomen, meer bepaald in advies nr. 07/2006 van 22 maart 2006 betreffende het project "monitoring kansengroepen" in het personeelsbestand van het Ministerie van de Vlaamse Gemeenschap beheerd via het Vlimpers-systeem en in advies nr. 05/2008 van 27 februari 2008 betreffende de monitoring van kansengroepen in de schoot van de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding.

Advies nr. 36/2012 van 12 december 2012

aangaande een voorontwerp van wet houdende sommige bepalingen van het administratief statuut van het operationeel personeel van de hulpverleningszones en boek 15 van een voorontwerp van koninklijk besluit tot bepaling van het administratief statuut van het operationeel personeel van de hulpverleningszone betreffende het uitvoeren van alcohol- en drugtests

Een brandweerman onder invloed van alcohol of drugs vormt een groot risico voor de veiligheid van hemzelf, zijn collega's en de burgers betrokken bij de interventies. Kan zijn werkgever objectieve vaststellingen doen aan de hand van alcohol- en drugtests en veiligheidsmaatregelen treffen. Bij een positieve test wordt het betrokken personeelslid uitgesloten van deelname aan de operationele opdrachten van de brandweer. Een personeelslid die medewerking aan de test weigert, kan eveneens preventief uitgesloten worden. Kan dit?

De werkgever van het brandweerpersoneel moet een preventiebeleid rond alcohol- en druggebruik uitwerken en toepassen ingevolge de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk (hierna "welzijnswet"). Voor de private sector kan bijkomend worden verwezen naar CAO nr. 100 van 1 april 2009 betreffende het voeren van een preventief alcohol- en drugbeleid in de onderneming.

De welzijnswet verplicht de werkgever de gezondheid, de veiligheid en het welzijn van zijn werknemers te garanderen. De werkgever is verplicht alle risico's te analyseren waaraan werknemers kunnen worden blootgesteld. Alcohol- en druggebruik houden risico's in voor de werknemer zelf, collega's en eventueel derden, bijgevolg moet de werkgever deze problematiek in zijn welzijnsbeleid opnemen.

Brandweerlieden vervullen een veiligheidsfunctie in de zin van artikel 2, 1° van het Koninklijk Besluit van 28 mei 2003 betreffende het gezondheidstoezicht op de werknemers, zodat zij een periodieke gezondheidsbeoordeling moeten ondergaan in beginsel jaarlijks.

Wat de toepasselijkheid van de Privacywet betreft, gaat het niet zozeer over de afname van de test zelf, maar de daaropvolgende verwerking van de testresultaten, bijvoorbeeld de opname ervan in het personeelsdossier.

De verwerking van testresultaten van alcohol- en drugtests door de brandweer is noodzakelijk te noemen voor de vervulling van de hem toevertrouwde taak van openbaar belang (cf. art. 5, e Privacywet) en desgevallend voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke voor de verwerking - mits het belang of de fundamentele rechten en vrijheden van de brandweerlieden niet zwaarder doorwegen (cf. art. 5, f Privacywet).

De doelstelling bestaat erin het nultolerantiebeleid ten aanzien van alcohol- en drugsgebruik tijdens de dienst te handhaven, dit in de eerste plaats om daaruit voortvloeiende risico's voor de werknemer zelf, collega's en eventueel derden te beheersen. Daarnaast moet ook de kwaliteit van de dienstverlening gewaarborgd blijven.

Dergelijke doelstelling is welbepaald, uitdrukkelijk omschreven en gerechtvaardigd.

Een individuele alcohol- of drugstest maakt geen medische handeling uit. In de gevallen dat de verwerking van de testresultaten een verwerking van gezondheidsgegevens uitmaakt, moet dit binnen het kader van artikel 7 Privacywet gebeuren. De werkgever die gedurende een periode meerdere alcohol- en/of drugstests afneemt bij een personeelslid, met de bedoeling na verloop van tijd zijn vermoedens te bekrachtigen (of te zien weerleggen) dat de betrokkene een alcohol- of drugsprobleem heeft, is bezig met de verwerking van gezondheidsgegevens in de zin van artikel 7 Privacywet. Doorslaggevend is niet het aantal tests dat afgenomen wordt, maar op welke wijze de resultaten gebruikt worden.

De werkgever mag slechts gebruik maken van alcohol- en drugtests voor zover zij reeds preventiebeleid hierrond voeren.

Een test mag enkel gevraagd worden indien de betrokkene kennelijke tekenen toont van hetzij alcoholintoxicatie, hetzij onder invloed te zijn van drugs. Blinde steekproeven zijn bijgevolg niet toegelaten.

De afname van een test en het gebruik van de testresultaten is enkel mogelijk voor personeel tijdens hun dienst. Personeelsleden die zich buiten deze situaties aanbieden kunnen niet tuchtrechtelijk vervolgd worden ingeval van een positieve test.

In alle omstandigheden moeten de testresultaten steeds met de nodige discretie behandeld worden en veilig bewaard worden overeenkomstig artikel 16 Privacywet.

Aanbeveling nr. 03/2013 van 24 april 2013
uit eigen beweging over het gebruik van traceertoestellen door politiediensten ten aan zien van hun personeelsleden

Reeds enkele jaren installeert de politie in zijn voertuigen traceertoestellen. Met deze apparatuur kunnen de voertuigen en dus de medewerkers gelokaliseerd worden of kunnen er gegevens worden ingewonnen en geanalyseerd over het gebruik van de voertuigen door deze medewerkers.

Finaliteit

Naast logistieke doeleinden (beheer wagenpark), operationele doeleinden (beheer van de interventies) en beveiligingsdoeleinden (voertuig kan niet starten zonder een activeringsbadge, wat belet dat het voertuig wordt gestolen), is er dus de vaststelling dat deze traceertoestellen ook met patronale controledoeleinden kunnen ingezet worden.

Met behulp van dergelijke toestellen kunnen de leden van de politiediensten inderdaad gecontroleerd worden op het gebruik dat ze gemaakt hebben van het voertuig (bruusk remmen, uren en duur van het gebruik, rijsnelheid, ongepast gebruik van zwaailichten, ...), maar ook hun komen en gaan (verplaatsingen). Daarnaast kunnen de beschikbare gegevens gebruikt worden – à charge of à decharge – bij een klacht over het gedrag van een lid van de politiediensten ten opzichte van een individu (bijvoorbeeld bij een ongeval, of laattijdige aankomst ter plaatse, ...).

Het doeleinde van controle op de personeelsleden verhindert dat er misbruik gemaakt wordt van het politiemateriaal, maar kan ook een bewijsmiddel opleveren in geval er een betwisting is rond het gedrag van een personeelslid.

Toelaatbaarheid

Volgens de Privacycommissie is het in het kader van een arbeidsrelatie niet zonder gevaar als de toestemming van de werknemer de basis vormt voor deze verwerking. In de arbeidscontext berust de toestemming niet op een evenwichtige machtsverhouding terwijl de Privacywet vereist dat een toestemming vrij zou zijn.

De Privacycommissie is van mening dat de verwerking van de gegevens wel toegelaten is krachtens artikel 5, f° van de Privacywet (het gerechtvaardigd prioritair belang van de verantwoordelijke voor de verwerking).

Proportionaliteit

De Privacycommissie verduidelijkt dat deze controle uitsluitend onder goed omkaderde omstandigheden mag gebeuren. De systematische en/of individuele controles mogen niet de grondnorm zijn en moeten een uitzondering blijven.

De analyse van de gegevens over het gedrag of de activiteiten van een personeelslid is slechts wettelijk als er ernstige aanwijzingen bestaan die een laakbaar, ongepast of verboden gedrag doen vermoeden, of als er bijzondere omstandigheden zijn die rechtvaardigen dat de verzamelde gegevens worden geraadpleegd, zoals klachten of aanwijzingen over misbruik tijdens politionele interventies, of het misbruik van politiematerieel (zwaailichten, sirenes, rijsnelheid, ...). De traceerfuncties moeten kunnen gedeactiveerd worden in het geval een personeelslid buiten de diensturen gebruik maakt van een dienstvoertuig, bijvoorbeeld wanneer hij het voertuig naar huis meeneemt omdat hij de dag erna ergens een werkvergadering heeft. Een tracering van dit voertuig buiten de diensturen kan als disproportioneel aanzien worden.

De Privacycommissie beveelt aan dat de gegevens verzameld door de traceersystemen niet worden aangewend voor permanente controles op de personeelsleden en dat een arbeidsreglement of een gelijkwaardig instrument het gebruik van gegevens voor controledoeleinden voldoende omkadert.

Transparantie

Indien de verzamelde gegevens zouden worden gebruikt om de activiteiten van een personeelslid van de politie te controleren voor disciplinaire doeleinden, moet de hiërarchische overste bij de aangifte van een incident waarbij een personeelslid betrokken is, dit personeelslid oproepen zodat hij hierover uitleg kan verschaffen. Een interpretatie van brute gegevens en het onmiddellijk opleggen van een sanctie zonder dat de betrokkene de mogelijkheid kreeg om zijn interpretatie van de hem betreffende traceergegevens te geven, zijn handelingen die niet alleen het principe van de tegensprekelijkheid aantasten maar ook artikel 12bis van de Privacywet (verbod op geautomatiseerde besluitvorming).

De Privacycommissie raadt aan om voor dit soort gegevensverwerking een voorafgaand overleg te houden met de personeelsvertegenwoordiging van de betrokken beroepsgroep zodat ook zij goed ingelicht zijn van de verwerking en de nagestreefde doeleinden.

Voor de materie inzake geolokalisatie in het algemeen kan eveneens worden gewezen op het oudere advies 12/2005 van 7 september 2005 betreffende het wetsvoorstel tot regeling van het toezicht op werknemers door middel van een monitoringsysteem verbonden met het GPS-navigatiesysteem van dienstwagens, waarin gelijklopende standpunten werden ingenomen, evenwel met uitzondering van de grondslag voor een dergelijke verwerking. In een advies nr. 12/2005 van 7 september 2005 werd nog gesteld dat de werknemer enkel gevolgd mag worden met behulp van een geolokalisatiesysteem, indien hij uitdrukkelijk toestemming heeft gegeven voor de installatie van dat systeem in zijn bedrijfswagen. Deze toestemmingsvereiste is verdwenen.

Advies nr. 18/2013 van 5 juni 2013
naar aanleiding van een klacht tegen de installatie van een kwaliteitsgarantieplatform om telefoongesprekken tussen werknemers en potentiële klanten van de werkgever op te nemen

In dit dossier werd door de klager bij de Privacycommissie een klacht ingediend tegen de opname en het beluisteren van professionele telefoongesprekken tussen werknemers en potentiële klanten van de werkgever.

Finaliteit

Het telefoonopnamesysteem van de werkgever houdt hoofdzakelijk in dat per Belgische winkel elke maand 50% van de reële inkomende gesprekken van prospecten (zij die zich voor het eerst als nieuwe klant melden) opgenomen wordt, waarvan er enkele nadien worden beluisterd en geëvalueerd op hun kwaliteit (nagaan of en de mate waarin het winkelpersoneel zich houdt aan het uitgeschreven verkoopscript) om op basis daarvan te bepalen of training/coaching van het winkelpersoneel aangewezen is.

Toelaatbaarheid

De registratie van de medewerkers is toegelaten op grond van de Arbeidsovereenkomstenwet van 3 juli 1978 dat het gezagsrecht van de werkgever verankert (o.a. in artikel 17). Deze wet vormt een wettelijke uitzondering op artikelen 314bis Strafwetboek en 124 van de wet van 13 juni 2005 betreffende de elektronische communicatie, en biedt een grondslag voor verwerking in de zin van artikel 5, c) Privacywet (verwerking toegelaten door de wet), in zoverre is voldaan aan de wet van 8 april 1965 betreffende de arbeidsreglementen. De Privacycommissie wijst erop dat ook bepaalde rechtsleer en rechtspraak al heeft erkend dat de artikelen 2, 3 en 17, 2° uit de Arbeidsovereenkomstenwet op zich een wettelijke toelating vormen om van de verbodsbepalingen van artikel 314bis Strafwetboek en artikel 124 van de telecomwet van 13 juni 2005 af te wijken en dat het de werkgever dus toegestaan is om, onder bepaalde voorwaarden, bijvoorbeeld kennis te nemen van de inhoud van telefoongesprekken tussen zijn werknemers en derden (waaraan hij niet deelneemt).

Het opnamesysteem viseert de telefonische gesprekken die de medewerker voert (met name deze met bellende prospecten) in het kader van de uitvoering van zijn arbeidsovereenkomst met de werkgever. Er kan dus gesteld worden dat het gaat om een verwerking in de zin van artikel 5, b) Privacywet (verwerking voor de uitvoering van een overeenkomst).

De registratie van de prospect is toegelaten, want berust in theorie op zijn toestemming in de zin van artikel 5, a) Privacywet. Indien de prospect niet wil dat het gesprek wordt opgenomen, zal de opgebelde werknemer de prospect vragen op een ander nummer terug te bellen of de code voor reeds bestaande cliënten in te toetsen (gesprek die niet wordt opgenomen). De prospect kan ook een winkel ter plekke bezoeken of de webapplicatie gebruiken.

Proportionaliteit

Het kunnen opnemen van werkelijke gesprekken en de analyse achteraf maakt coaching mogelijk op basis van “real life” experiences met een groter leereffect tot gevolg. De concrete omstandigheden en restricties onder dewelke die reële gesprekken worden geregistreerd, beluisterd en geëvalueerd verdragen zich in beginsel met de Privacywet: het gaat nooit over privégesprekken, het gaat enkel over een deel van de professionele gesprekken (met prospecten). Slechts de helft van bedoelde gesprekken worden geregistreerd, waarvan er slechts enkele nadien worden beluisterd en geëvalueerd op hun kwaliteit door een beperkt aantal personeelsleden van de werkgever om op basis daarvan te bepalen of training/coaching van het winkelpersoneel aangewezen is en zonder dat dit verder aanleiding kon geven tot een beloning of een sanctie. De retentieduur bedraagt maximaal 30 dagen.

De Privacycommissie voegt toe dat in de rechtspraak die toeliet dat de werkgever, onder bepaalde voorwaarden, kennis kon nemen van de inhoud van telefoongesprekken tussen zijn werknemers en derden (waaraan hij niet deelneemt), het steeds ging om de werkelijke controle door de werkgever van misbruik van materiaal dat aan de werknemers ter beschikking gesteld werd met mogelijke tuchtmaatregelen tegen de betrokken werknemers als gevolg.

Een systeem, zoals in voorliggend geval, waarbij het “slechts” gaat om een periodieke kwaliteitsopvolging van de relatie tussen de dienstverlening en de klant om op basis daarvan aangepaste operationele coaching en training aan te bieden, zonder dat aan deze kwaliteitscheck verdere sancties of beloningen verbonden zijn voor de werknemers, is duidelijk minder intrusief.

Transparantie

De personen die werkzaam zijn bij de werkgever en de personeelsvertegenwoordiging werden, vooraleer het systeem effectief werd ingevoerd, meermaals op de hoogte gebracht van de intentie om het bedoeld registratiesysteem te installeren, het precieze doel ervan en de duur van bewaring van de geregistreerde communicatie en gegevens.

Collectief arbeidsrecht

Derhalve kon door de Privacycommissie geen enkele inbreuk op de Privacywet worden vastgesteld of aangetoond, behoudens, vanuit

sociaalrechtelijk oogpunt, de niet opname van het systeem in het arbeidsreglement. Het registratiesysteem werd inderdaad ingevoerd zonder enige voorafgaande vermelding in het arbeidsreglement, zoals nochtans vereist door artikel 6, § 1, 5° van de wet van 8 april 1965 betreffende de arbeidsreglementen.

Aanbevelingen

Behoudens de niet opname in het arbeidsreglement op het moment van de invoering, bevestigt de Privacycommissie dus de algemene legitimiteit van het systeem, maar vraagt de werkgever toch volgende bijkomende waarborgen na te leven bij de herinvoering van het naar aanleiding van de klacht opgeschorte systeem:

- waarborg dat de werkgever het systeem evalueert in de tijd en eventueel herziet in functie van toekomstige ontwikkelingen;
- waarborg dat de ondernemingsraad het systeem kan evalueren in de tijd en voorstellen kan doen met het oog op eventuele herziening in functie van toekomstige ontwikkelingen;
- waarborg dat de ondernemingsraad een blik gegund blijft "onder de motorkap" van het systeem;
- waarborg dat de werkgever de gegevens te goeder trouw en in overeenstemming met het eraan gegeven doeleinde verwerkt; dat elk hergebruik verenigbaar is met het oorspronkelijke doeleinde in de zin van artikel 4, § 1, 2° Privacywet en dat alle maatregelen genomen worden om interpretatiefouten op dat vlak te vermijden;
- waarborg dat de gesprekken effectief willekeurig worden beluisterd en geselecteerd door een beperkt aantal personeelsleden van de werkgever;
- waarborg dat er effectief vorming/training volgt op evaluaties van gesprekken die reële;
- leerpunten blootleggen;
- waarborg dat de beslissing tot vorming/training niet uitsluitend is gebaseerd op gegevens die via het systeem verkregen werden;
- waarborg dat gesprekken die niet valabel blijken te zijn voor verdere analyse en evaluatie eerder dan de thans voorziene 30 dagen worden gewist uit het systeem;
- waarborg dat indien andere gesprekken dan met bellende prospecten zouden worden;
- opgenomen, deze zo spoedig mogelijk uit het opnamesysteem worden geweerd;
- waarborg dat winkelmedewerkers ook op hun andere (en hoofdzakelijke) werkprestaties die zij verrichten in uitvoering van hun arbeidsovereenkomst worden beoordeeld;
- waarborg dat de evaluaties van de opgenomen gesprekken met prospecten niet meer;
- zouden mogen worden gewijzigd (maar enkel geraadpleegd) eenmaal de opgenomen;
- gesprekken zijn gewist uit het systeem en dit om discussies te vermijden;
- waarborg dat het systeem in het arbeidsreglement wordt opgenomen.

Advies nr. 65/2013 van 18 december 2013 betreffende een voorontwerp van decreet betreffende de opvang van kinderen tot twaalf jaar

Dit advies heeft betrekking op een voorontwerp van decreet betreffende de opvang van kinderen tot twaalf jaar (hierna het voorontwerp).

Het voorontwerp legt het kader voor de erkenning van kinderopvang en het toezicht erop. Het voorontwerp regelt ook een aantal verwerkingen van persoonsgegevens door de dienstverrichters die kinderopvang aanbieden, nl. medische attesten met betrekking tot hun personeel (en soms gezinsleden) en uittreksels uit het strafregister met betrekking tot hun personeel.

De personen die werkzaam zijn in de kinderopvang moeten een uittreksel uit het strafregister kunnen overleggen waaruit blijkt dat ze een activiteit kunnen uitoefenen op het gebied van opvoeding, psycho-medisch-sociale begeleiding, jeugdbijstand, kinderbescherming, animatie of begeleiding van minderjarigen; het gaat daarbij om "model 2" van het uittreksel uit het strafregister.

Uit het voorontwerp leidt de Privacycommissie af dat het uittreksel uit het strafregister zowel door de toezichthoudende overheid als door de dienstverrichter zelf bewaard zal worden. Voor het behoud van de erkenning moet de dienstverrichter immers op elk moment kunnen aantonen dat de erkenningsvoorwaarden bepaald in het voorontwerp vervuld zijn.

Het uittreksel uit het strafregister en zijn inhoud vormen gerechtelijke gegevens in de zin van artikel 8 Privacywet. Het voorontwerp creëert een decretale basis om de verwerking van deze gerechtelijke gegevens te rechtvaardigen met als doel kinderopvang enkel toe te vertrouwen aan personen met een onberispelijk gedrag in de omgang met kinderen.

De verwerking van deze gerechtelijke gegevens dient met respect voor het proportionaliteitsbeginsel te gebeuren. De gegevens mogen enkel toegankelijk zijn voor personen die ze nodig hebben voor de uitoefening van hun taken.

De personen die in de kinderopvang werkzaam zijn dienen bovendien te beschikken over een medisch attest dat bevestigt dat hun gezondheidstoestand hen toelaat voor kinderen te zorgen. Vrouwen

werkzaam in de kinderopvang dienen een medisch attest te bezorgen dat zij gevaccineerd zijn tegen rodehond. Vaccinatie tegen rodehond kan enkel achterwege blijven mits voorlegging van een gemotiveerd medisch attest.

Het voorontwerp creëert een decretale basis voor de verwerking van deze gezondheidsgegevens. Gelet op de verantwoordelijkheid die rust op dienstverrichters en personen die in de kinderopvang werkzaam ten aanzien van de opgevangen kinderen, en wat rodehond betreft de bescherming van nog ongeboren kinderen, acht de Privacycommissie het beoogde doel inderdaad zwaarwegend.

In deze specifieke arbeidssetting (werkzaamheden in de kinderopvang), ziet de Privacycommissie dus geen a priori bewaar in de verwerking door de werkgever van gerechtelijke en gezondheidsgegevens van personeelsleden.

Commissie voor de bescherming van de persoonlijke levenssfeer

Drukpersstraat 35 | B-1000 Brussel | **T**+32 (0)2 274 48 00 | **E-mail** commission@privacycommission.be | **Website** www.privacycommission.be

Verantwoordelijke uitgever: W. Debeuckelaere | Publicatiedatum: Januari 2015

Er bestaat ook een Franse versie van deze brochure. | Il existe aussi une version française de cette brochure.