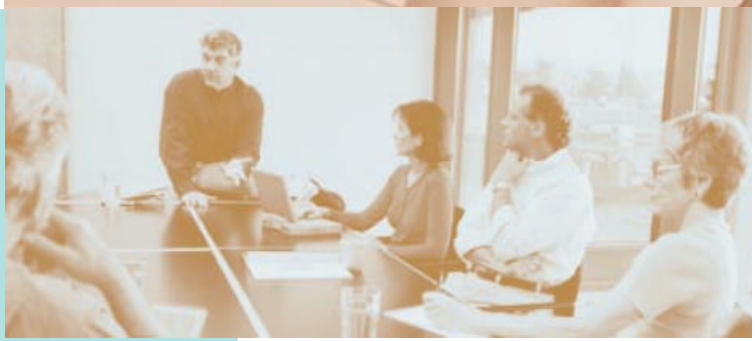
LLEGE BESCHERMING
RSOONSGEGEVENS
liana van Stolberglaan
10
ostbus 93374
509 AJ Den Haag
LEFOON 070 888 85 00
X 070 888 85 01
MAIL info@cbpweb.nl
TERNET www.cbpweb.nl

Privacy: checklist voor de ondernemingsraad

INHOUD



COLOFON
April 2002
Uitgave: College bescherming persoonsgegevens
Bewerker: mr. M.Th. van Munster-Frederiks
Grafisch ontwerp: Proforma, strategie, ontwerp en management
Druk: Sdu Grafisch Bedrijf

COLLEGE | BESCHERMING | PERSOONSGEGEVENS

DE ONDERNEMINGSRAAD DIENT DOOR DE ONDERNEMER BETROKKEN TE WORDEN BIJ REGELINGEN VOOR HET VERWERKEN VAN PERSOONSGEGEVENS EN HET GEBRUIK VAN PERSONEELS-VOLGSYSTEMEN. DE ONDERNEMINGSRAAD HEEFT DE PLICHT ZIJN INSTEMMINGSRECHT VOOR DEZE VERWERKINGEN UIT TE OEFENEN.

INHOUDSOPGAVE

VOORWOORD

Ondernemingsraden spelen bij de privacybescherming van medewerkers op de werkplek een cruciale rol. De Wet op de Ondernemingsraden bepaalt dat een ondernemer de instemming van de ondernemingsraad nodig heeft als hij regelingen voor persoonsgegevens van medewerkers wil verwerken.

Per 1 september 2001 is de Wet bescherming persoonsgegevens in werking getreden als de opvolger van de Wet Persoonsregistraties. Reden voor het College bescherming persoonsgegevens om de "Checklist voor ondernemingsraden", die gebaseerd was op de Wet Persoonsregistraties, aan te passen aan deze nieuwe wet.

Aan de hand van 25 toetsingsvragen met voorbeelden worden de belangrijkste voorwaarden besproken voor het behoorlijk, zorgvuldig en rechtmatig omgaan met persoonsgegevens van medewerkers op het werk.

Als de organisatie een functionaris voor de gegevensbescherming heeft aangesteld, kan deze interne toezichthouder ook de ondernemingsraad met advies ter zijde staan.

Het College wil met deze privacychecklist ondernemingsraden een handreiking bieden bij het realiseren van een passend niveau van privacybescherming in bedrijven en organisaties.

Ik wens u daarbij veel succes.

mr. P.J. Hustinx
Voorzitter

< VORIGE INHOUD VOLGENDE >

1

PRIVACY, PERSOONSGEGEVENS EN DE ONDERNEMINGSRAAD

De ondernemingsraad (OR) is nauw betrokken bij afspraken over de verwerking van personeelsgegevens en personeelsvolgsystemen in een onderneming.

De in artikel 27 van de Wet op de ondernemingsraden (WOR) geregelde verplichte instemming van de OR met betrekking tot voorgenomen besluiten is per 4 maart 1998 uitgebreid.
De OR dient sindsdien ook te oordelen over twee soorten besluiten die de persoonlijke levenssfeer van medewerkers raken. De beoordeling door de OR betreft voorgenomen besluiten tot vaststelling, wijziging of intrekking van twee soorten regelingen:

a Regelingen inzake het verwerken van alsmede de bescherming van de persoonsgegevens van de personen die in de onderneming werkzaam zijn (geregeld in artikel 27, eerste lid onder k. van de WOR en aangepast aan de Wet bescherming persoonsgegevens via de Aanpassingswet van 5 april 2001).

b Regelingen inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de personen die in de onderneming werkzaam zijn (of wel personeelsvolgsystemen geregeld in artikel 27, eerste lid onder l. van de WOR).

De OR draagt dus medeverantwoordelijkheid voor de omgang met en de bescherming van persoonsgegevens op het werk. Om ondernemingsraden een handreiking te bieden bij de afwegingen die rond het verwerken van persoonsgegevens gemaakt moeten worden, heeft het College bescherming persoonsgegevens een checklist ontwikkeld. De checklist wordt in deze brochure uitvoerig toegelicht, voorafgegaan door een schets van de Wet bescherming persoonsgegevens op hoofdpunten.

In de checklist en de toelichting daarop worden de begrippen ‘ondernemer(s)’ en ‘medewerker(s)’ gehanteerd. Voor het begrip ondernemer is aansluiting gezocht bij de definitie in artikel 1, eerste lid onder d. van de WOR: de natuurlijke persoon of de rechtspersoon die een onderneming in stand houdt. Met het begrip medewerker(s) wordt bedoeld de in de onderneming werkzame perso(o)nen in de zin van artikel 2 van de WOR. De WOR is van toepassing op zowel het bedrijfsleven als de overheidsdiensten.

De checklist begint met een aantal algemene toetsingsvragen om te beoordelen of er inderdaad sprake is van verwerking van persoonsgegevens en van personeelsvolgsystemen volgens de Wet bescherming persoonsgegevens (WBP).

Specifieke toetsingsvragen voor verwerking van persoonsgegevens zoals de ondernemer deze wil laten verrichten, maken vervolgens het grootste deel van de privacychecklist uit.

Personeelsvolgsystemen zijn bijzondere gevallen van de verwerking van persoonsgegevens. Hierbij moet een OR niet te snel denken dat deze niet in de onderneming voorkomen want ook systemen die geschikt zijn om personeel te volgen, vallen hieronder. De checklist sluit af met specifieke toetsingsvragen voor deze verwerkingen.

< VORIGE | INHOUD | VOLGENDE >

2 DE WET BESCHERMING PERSOONSGEGEVENS

Het wettelijk kader voor de omgang met persoonsgegevens is vastgelegd in de Wet bescherming persoonsgegevens (WBP). Deze wet is sinds 1 september 2001 van kracht en is de opvolger van de Wet persoonsregistraties. Voor het rechtmatig verwerken van persoonsgegevens en het zorgvuldig en behoorlijk omgaan met persoonsgegevens schrijft de WBP een aantal dwingende normen voor. Deze normen zijn uitgewerkt in een aantal basisvoorwaarden.

1 Doelbinding
Persoonsgegevens (dat zijn alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon) mogen slechts voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor doeleinden die daarmee onverenigbaar zijn.

2 Rechtmatige grondslag
De verwerking van persoonsgegevens (dat is elke handeling die met persoonsgegevens verricht kan worden) moet berusten op een in de WBP genoemde grondslag, zoals toestemming, overeenkomst, wettelijke plicht, gerechtvaardigd belang van het bedrijf of de organisatie. Voor bijzondere gegevens (godsdienst, ras, politieke gezindheid, gezondheid, seksuele geaardheid, lidmaatschap van een vakvereniging, strafrechtelijke gegevens en gegevens over onrechtmatig of hinderlijk gedrag waarvoor een verbod is opgelegd) gelden striktere normen.

3 Kwaliteit
De persoonsgegevens moeten zoveel mogelijk juist, nauwkeurig, toereikend, ter zake dienend en niet bovenmatig zijn.

4 Transparantie
De betrokkene (dat is de persoon wiens persoonsgegevens worden verwerkt) moet kunnen overzien door wie en voor welk doel zijn gegevens worden verwerkt.

5 Melden: voornemen en verwerking
De verwerking van persoonsgegevens moet vooraf worden gemeld bij het College bescherming persoonsgegevens (CBP) of een functionaris voor de gegevensbescherming, tenzij de verwerking daarvan is vrijgesteld. Van bepaalde persoonsgegevens moet ook al het plan (voornemen) deze te verwerken gemeld worden met het oog op een beoordeling door het CBP (voorafgaand onderzoek).

6 Rechten van de betrokkenen
De betrokkenen hebben het recht om kennis te nemen van hun gegevens en om te verzoeken deze te laten verbeteren of te laten verwijderen. Tevens hebben zij er recht op om bezwaar te maken tegen het verwerken van persoonsgegevens.

7 Beveiliging
Passende maatregelen van technische en organisatorische aard vormen het noodzakelijke sluitstuk van een rechtmatige verwerking.

8 Verwerking door een bewerker
Als de verwerking wordt uitbesteed aan een bewerker, moet worden verzekerd dat deze zich houdt aan de aanwijzingen van de verantwoordelijke.

9 Gegevensverkeer met landen buiten de Europese Unie
Het verkeer van persoonsgegevens naar een land buiten de Europese Unie (EU) is in principe alleen toegestaan als dat land een passend niveau van bescherming heeft. Al deze basisvoorwaarden voor de verwerking van persoonsgegevens zijn verwerkt in de hierna volgende toetsingsvragen.

3 k ALGEMENE TOETSINGSVRAGEN

Volgens de omschrijving in artikel 27, eerste lid, onder k. van de WOR is het instemmingsrecht van toepassing ten aanzien van een voorgenomen besluit van de ondernemer inzake de vaststelling, wijziging of intrekking van een regeling omtrent het verwerken van alsmede de bescherming van persoonsgegevens van de in de onderneming werkzame personen. Hiermee wordt in de praktijk een regeling bedoeld omtrent de verwerking van persoonsgegevens. Voor de interpretatie van de begrippen 'persoonsgegeven' en 'verwerking' moet worden gekeken naar de WBP.

1 Is sprake van een persoonsgegeven?

Een persoonsgegeven in de zin van de WBP is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het kan om allerlei soorten informatie gaan: om eigenschappen van de betrokkene, diens opvattingen of gedragingen. Meer in het algemeen gaat het om gegevens die bepalend kunnen zijn voor de manier waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.

Voorbeelden van persoonsgegevens zijn:

- naam, adres, sofi-nummer (het 'administratieve schaduw-beeld')
- een video-opname van een persoon
- gegevens over iemands telefoon- of computergebruik
- het kentekennummer of het benzineverbruik van een lease-auto
- iemands ziekteverzuim en de redenen daarvan
- een registratie van gevolgde cursussen en opleidingen in het kader van carrièreverloop
- biometrische gegevens (b.v. irisscan, vingerafdruk).

Van een persoonsgegeven is pas sprake als de identiteit van de persoon op wie de informatie betrekking heeft, ook redelijkerwijs kan worden vastgesteld. Dit betekent dat de informatie individualiseerbaar moet zijn. Of gegevens individualiseerbaar zijn, wordt bepaald door de grenzen van wat redelijkerwijs binnen de mogelijkheden van de onderneming ligt of wat met behulp van aanvullende informatie achterhaald kan worden. Zodra gegevens tot één of meer betrokken medewerkers te herleiden zijn, zal al snel sprake zijn van persoonsgegevens. De omvang van een bepaalde afdeling kan er dus toe doen. Een personeelsnummer in een bedrijf is tot een persoon te herleiden. Ook met behulp van een login-naam is een medewerker te traceren

Geen persoonsgegevens zijn bijvoorbeeld:

- de getotaliseerde gegevens over het personeelsbestand van een bedrijf met een redelijke omvang of
- de geaggregeerde (dat wil zeggen gegroepeerde, niet tot een individuele medewerker te herleiden) gegevens over het telefoongebruik binnen een onderneming.

2 Is sprake van verwerking van persoonsgegevens?

De WBP kent het ruime begrip 'verwerking van persoonsgegevens'. Hieronder wordt verstaan elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder het geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

< VORIGE INHOUD VOLGENDE >

Op de in artikel 27, eerste lid, onder k. van de WOR genoemde verwerkingen is de WBP van toepassing als de gegevens geheel of gedeeltelijk geautomatiseerd worden verwerkt. Ook is de WBP van toepassing op persoonsgegevens die in een bestand zijn opgeslagen. Denk hierbij ook aan handmatig bijgehouden bestanden. Van een bestand is sprake bij structurering en een bepaalde mate van toegankelijkheid van de gegevens.

3 Wie is de verantwoordelijke?

De verantwoordelijke is degene die beslist of, en zo ja, welke gegevens worden verwerkt, met welk doel dat gebeurt en op welke wijze. Het gaat primair om degene die formeel-juridisch de zeggenschap heeft. Meestal is dit de rechtspersoon. Als dit onvoldoende duidelijk is, moet gekeken worden naar het tweede criterium: degene aan wie de verwerking naar de maatstaven die in het maatschappelijk verkeer gelden, moet worden toegerekend. Bij concernverhoudingen is bepalend onder wiens bevoegdheid de operationele gegevensverwerking plaats vindt. De feitelijke macht of invloed van een andere rechtspersoon binnen het concern is niet van belang.

In de WOR is geregeld wat onder onderneming, ondernemer en bestuurder moet worden verstaan. In zijn algemeenheid kan gesteld worden dat de ondernemer in de zin van de WOR gezien kan worden als de verantwoordelijke in het kader van de WBP.

Bij een concern zal iedere dochtermaatschappij op zich de verantwoordelijke zijn. Dit betekent dat personeelsgegevens niet zomaar verstrekt mogen worden aan bijvoorbeeld de Raad van Bestuur van het concern of een staf-afdeling van het concern. Daarvoor moet een goede en rechtsgeldige reden zijn.

Als de verantwoordelijke niet zelf persoonsgegevens verwerkt maar de feitelijke handelingen laat verrichten door een daarin gespecialiseerde organisatie (bijvoorbeeld een salaris-administratiebureau), dan is deze organisatie een zogenaamde 'bewerker'. De WBP stelt eisen aan vorm en inhoud van de afspraken die de verantwoordelijke met een bewerker maakt. De verantwoordelijke kan altijd aansprakelijk worden gesteld voor een onrechtmatige verwerking. De bewerker is zelfstandig aansprakelijk voor gebreken binnen zijn organisatie.

4 Kan de OR gebruik maken van het instemmingsrecht?

Wanneer de ondernemer van plan is een besluit te nemen tot vaststelling, wijziging of intrekking van een regeling ten aanzien van de verwerking van persoonsgegevens of een personeelsvolgsysteem heeft de OR de plicht zijn instemmingsrecht uit te oefenen.
Iedere ondernemer zal na 1 september 2001 tenminste een aantal besluiten moeten nemen in verband met de administratieve verplichtingen op grond van WBP zoals de melding van de verwerkingen van persoonsgegevens bij het CBP of bij de functionaris voor de gegevensbescherming. Daarbij zal de OR betrokken moeten worden. De melding hoeft niet plaats te vinden als de gegevensverwerking is vrijgesteld op grond van het Vrijstellingsbesluit.

De OR kan eventueel een beroep doen op het initiatiefrecht van artikel 23 van de WOR wanneer de ondernemer, in de ogen van de OR, niet de noodzakelijke actie onderneemt.

In het geval dat de OR niet instemt met het voorgenomen besluit van de ondernemer, kan de ondernemer de kantonrechter om toestemming vragen (artikel 27, vierde lid WOR).

< VORIGE INHOUD VOLGENDE >

4

TOETSINGSVRAGEN VOOR DE VERWERKING VAN PERSOONSGEGEVENS

Alvorens in te stemmen met een regeling voor de verwerking van persoonsgegevens kan de regeling krachtens artikel 27, eerste lid onder k. van de WOR op de volgende punten worden getoetst.

5 Worden de persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt?

De hoofdregel van de WBP eist dat persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de wet worden verwerkt.

Dat gegevens in overeenstemming met de wet moeten worden verwerkt, betekent niet alleen dat de ondernemer zich aan de WBP moet houden. Hij moet zich ook houden aan andere relevante regelgeving waarin bijzondere regels voor gegevensverwerking zijn opgenomen (bijvoorbeeld de sociale verzekeringswetgeving of de wet SAMEN).

6 Voor welk doel worden de persoonsgegevens verwerkt?

De ondernemer (verantwoordelijke) moet de doelen bepalen vóórdat hij begint met het verwerken van persoonsgegevens. Hierbij is van belang dat het doel van de verwerking zo nauwkeurig en volledig mogelijk wordt omschreven. Als er meerdere doelstellingen zijn, moeten deze afzonderlijk worden genoemd en getoetst op de noodzaak om met het oog hierop persoonsgegevens te verzamelen.

Doel van het verwerken is bijvoorbeeld het registreren van toetsaanslagen op de computer per tijdseenheid ter voorkoming van de zogenaamde 'muisarm'. Of is het doel ook de productie van de medewerker op de computer vast te stellen? Wordt het telefoongebruik alleen maar geregistreerd met het oog op kostenbeheersing of ook om de productie te meten? Vinden video-opnamen alleen plaats ter beveiliging van medewerkers en eigendommen of ook om de medewerkers te observeren bij het uitvoeren van hun werkzaamheden?

7 Wanneer mogen persoonsgegevens verwerkt worden?

Verwerking van persoonsgegevens mag alleen plaatsvinden op een of meer van de volgende gronden. Deze zijn:

a Ondubbelzinnige toestemming;
b Noodzakelijk voor de uitvoering van een overeenkomst;
c Noodzakelijk voor de nakoming van een wettelijke verplichting;
d Noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene;
e Noodzakelijk voor een goede vervulling van een publiekrechtelijke taak;
f Noodzakelijk voor de behartiging van een gerechtvaardigd belang van de ondernemer ñ terwijl de persoonlijke levenssfeer van de betrokkenen niet prevaleert.

Ook al staat de toestemming voorop, vaak zal de grondslag voor de verwerking een andere zijn. In veel gevallen vloeit de verwerking voort uit een arbeidsovereenkomst (grondslag b) of wordt deze voorgeschreven door de overheid (grondslag c), bijvoorbeeld in het kader van de uitvoering van de sociale zekerheid.

Vrijwaring van een vitaal belang (grondslag d) zal in de praktijk weinig voorkomen. Het moet gaan om een zaak van 'leven of dood' die ook nog spoedeisend moet zijn. De grondslag genoemd onder e) heeft vooral betrekking op de situatie dat een bestuursorgaan gegevens moet verwerken om zijn publiekrechtelijke taak op een goede manier te kunnen uitoefenen of dat een bedrijf of organisatie informatie met het oog hierop aan een bestuursorgaan moet verstrekken. Vaak vindt samenloop met de wettelijke plicht tot verstrekking vangegevens plaats. Ook kunnen er gerechtvaardigde belangen voor een ondernemer zijn om gege-

< VORIGE | INHOUD | VOLGENDE >

vens over zijn medewerkers te verwerken (grondslag f), bijvoorbeeld maatregelen in het belang van de bedrijfsveiligheid of de bescherming van bedrijfsbelangen.

De privacybelangen van de betrokken medewerkers dienen in dit geval altijd tegenover de belangen van de ondernemer uitdrukkelijk worden afgewogen. Ook al heeft de ondernemer een gerechtvaardigd belang om persoonsgegevens te verwerken dan nog kan het zo zijn dat verwerking achterwege moet blijven vanwege een klemmend belang van privacybescherming van medewerkers. Het bieden van een bezwaarmogelijkheid kan aan de belangen van de medewerkers tegemoet komen.

De ondubbelzinnige toestemming (grondslag a) van de betrokken medewerker functioneert in de praktijk als een restcategorie. Deze toestemming mag niet verward worden met de instemming van de OR. Ook al heeft de OR zijn instemming aan een bepaalde verwerking gegeven, de toestemming van de individuele medewerker blijft noodzakelijk als deze grond van toepassing is.

8 Blijft het gebruik van de persoonsgegevens beperkt tot de doelen waarvoor de gegevens werden verzameld?

Natuurlijk mogen gegevens worden gebruikt voor de doeleinden die hiervoor zijn vastgesteld. Maar het is niet zo dat ander gebruik in het geheel niet is toegestaan. Onder de WBP is verdergaand gebruik toegestaan op voorwaarde dat dit ëniet onverenigbaarí is met het doel waarvoor de gegevens zijn verzameld.

Criteria voor het beoordelen hiervan zijn onder meer:

a De verwantschap tussen het doel van de door de ondernemer gewenste verwerking van de persoonsgegevens en het doel waarvoor deze zijn verkregen;
b De aard van de gegevens;
c De gevolgen van de verwerking voor de betrokken medewerker;
d De wijze waarop de gegevens zijn verkregen;
e De waarborgen waarmee het verdergaande gebruik wordt omgeven.

Om te kunnen beoordelen of in een concreet geval sprake is van verenigbaar gebruik, moeten deze factoren in onderling verband worden beoordeeld. Van belang is om de gevolgen voor de medewerker in te schatten. Voorts kan het uitmaken of de gegevens door de medewerker verplicht zijn aangeleverd of vrijwillig zijn verstrekt.

'Verenigbaar' met het doel waarvoor de persoonsgegevens in het kader van de arbeidsverhouding zijn vastgelegd is het verzorgen van een mailing in het kader van een employee benefits-programma. 'Niet verenigbaar' met het doel van een verzekerdenadministratie is het verstrekken van informatie over de arbeidsongeschiktheid van een medewerker door een ondernemer die tevens assurantiepersoon is, in een ontslagprocedure bij de kantonrechter.

9 Wordt volstaan met zo min mogelijk persoonsgegevens?

Een belangrijk uitgangspunt van privacybescherming is dat zo min mogelijk persoonsgegevens worden verwerkt. Alleen die persoonsgegevens die nodig zijn om het doel te bereiken, mogen worden verwerkt. Het minimum aan persoonsgegevens is daarom ook meteen het maximum.

De OR kan de volgende vragen stellen:

a Wordt voldoende gebruik gemaakt van de mogelijkheden van anonimisering, versleuteling, codering van gegevens?
b Moeten de gegevens op individueel niveau worden verzameld of kan worden volstaan met gegevens op het niveau van een afdeling of van het bedrijf als geheel (geaggregeerd niveau)?
c Moeten over alle personeelsleden gegevens worden vastgelegd of kan worden volstaan met het verzamelen van informatie over medewerkers in bepaalde functies of op bepaalde plaatsen?
d Kan worden volstaan met een steekproef of moeten voortdurend gegevens worden vastgelegd? Of gaat het juist om bepaalde personeelsleden?

In het doel van de personeelsadministratie van een wereldwijd concern kan ook besloten liggen de verspreiding van informatie over 'skills' van de medewerkers binnen het concern in het kader van loopbaanontwikkeling en detachering. In eerste instantie is voor het maken van een selectie de naam van de medewerker niet relevant. Informatie over 'skills' kan dus anoniem worden aangeboden. Pas als een dochtermaatschappij geïnteresseerd is, kan ook de naam van de medewerker worden verstrekt.

10 Zijn voldoende maatregelen genomen om te waarborgen dat de persoonsgegevens juist en nauwkeurig zijn?

Persoonsgegevens waarop medewerkers worden beoordeeld en op grond waarvan beslissingen worden genomen, moeten

toereikend, ter zake dienend en niet bovenmatig zijn. De ondernemer moet maatregelen treffen om te waarborgen dat de gegevens juist en nauwkeurig zijn.

De ondernemer kan regelmatig een overzicht van de gegevens verstrekken aan de medewerkers met het verzoek deze op juistheid te controleren. Hierbij zijn niet alleen adresgegevens, etc. in de personeelsadministratie van belang maar bijvoorbeeld ook de aanwezigheidsregistratie. Na maanden weet een medewerker vaak niet meer op welke dagen hij hoeveel uur heeft gewerkt, maar na een week nog wel. Hetzelfde geldt voor registratie van de productie. De wijze van verzamelen dient dus de nauwkeurigheid en juistheid van de gegevens te bevorderen.

11 Worden persoonsgegevens zoveel mogelijk verzameld bij de medewerker zelf?

De medewerker is doorgaans de eerste bron voor gegevens. Soms zal een ander ook zonder toestemming gegevens over een medewerker mogen verstrekken aan de ondernemer. De medewerker dient er wel van op de hoogte te zijn als dit gebeurt.

Hierbij kunnen door de OR bijvoorbeeld de volgende vragen worden gesteld:

a Wordt de medewerker als eerste gevraagd om gegevens waarover hij zelf de beschikking heeft?
b Weet hij wanneer gegevens over hem worden verzameld bij derden?

12 Hebben slechts die personen toegang tot persoonsgegevens die de gegevens nodig hebben voor de vervulling van hun taak?

Doorgaans mogen persoonsgegevens alleen worden gebruikt door bepaalde functionarissen en alleen maar ten aanzien van medewerkers met wie zij te maken hebben: denk aan de afdeling Personeel & Organisatie / Human Resource Management en lijnchefs. De verspreiding van persoonsgegevens moet aan banden worden gelegd.

Niet toegestaan is bijvoorbeeld:
Het plaatsen van gegevens over het ziekteverzuim van individuele medewerkers op het prikbord in de hal, of het met naam en toenaam noemen van veroorzakers van bedrijfsongevallen in het bedrijfsinfobulletin. In het kader van het veiligheidsbeleid is dat niet nodig, wel het benoemen van het ongeval en de oorzaken.

13 Worden gegevens ook aan personen buiten de onderneming verstrekt?

Voor het verstrekken van persoonsgegevens wordt in de WBP geen onderscheid gemaakt of dit voor intern (binnen de onderneming) of extern (buiten de onderneming) gebruik is. Gesteld kan worden dat dezelfde afwegingen gelden voor zowel intern als extern gebruik (zie hiervoor toetspunt 7). De afgrenzing ligt ook in het begrip verantwoordelijke (zie toetsingsvraag 3).

Als de ondernemer op grond van een gerechtvaardigd belang personeelsgegevens aan een derde verstrekt, moet een afweging worden gemaakt tussen het bedrijfsbelang en het privacybelang van de medewerker. Omdat bij extern gebruik de kans op inbreuk in de persoonlijke levenssfeer van de medewerker groter is dan bij intern gebruik, zullen in de praktijk de waarborgen in dat geval ook groter moeten zijn.

Aan de uitvoeringsinstelling voor de uitkering van sociale verzekeringen mogen persoonsgegevens van medewerkers worden verstrekt. Ook kunnen in het kader van de arbeidsvoorwaarden zogenaamde employee benefits-afspraken gemaakt zijn die gegevensverstrekking aan bijvoorbeeld een assurantietussenpersoon meebrengen. Ook bij het verstrekken van persoonsgegevens binnen een concern zal deze verstrekking getoetst moeten worden aan de rechtmatigheidgronden genoemd in toetspunt 7.

14 Vindt gegevensverkeer naar het buitenland plaats?

Hier moet onderscheid worden gemaakt tussen gegevensverkeer binnen de Europese Unie (EU) en buiten de EU.
De WBP kent geen aparte bepalingen voor gegevensverkeer binnen de Europese Unie. Op basis van de Europese privacyrichtlijn is binnen de EU-lidstaten een gelijkwaardige bescherming van persoonsgegevens tot stand gebracht en vrij verkeer van persoonsgegevens mogelijk gemaakt. Gegevensverkeer van Nederland naar een ander EU-land hoeft alleen te voldoen aan de algemene vereisten van de WBP.

Voor gegevensverkeer naar landen buiten de EU, de zogenaamde derde landen, gelden specifieke bepalingen.

De personeelsgegevens van een Nederlandse dochtermaatschappij of de vaardigheidsgegevens van de medewerkers mogen niet zonder meer worden opgeslagen in de centrale database van de moedermaatschappij in de Verenigde Staten.

< VORIGE INHOUD VOLGENDE >

De hoofdregel is dat persoonsgegevens alleen mogen worden doorgegeven naar een derde land als voldaan is aan de algemene vereisten van de WBP én het derde land een passend beschermingsniveau waarborgt.

Om vast te stellen of dit het geval is, moet de verantwoordelijke eerst nagaan of er een besluit is van de Minister van Justitie of van de Europese Commissie waarin iets wordt bepaald over het niveau van bescherming in een derde land. Is er geen besluit dan moet een verantwoordelijke zelf aan de hand van de relevante wettelijke regelingen een analyse van de situatie maken. Op de CBP-website is een lijst met landen te vinden waar de Europese Commissie een besluit over heeft genomen. Deze lijst bevat de landen waar een passend niveau van bescherming aanwezig wordt geacht.

Als een derde land geen passend beschermingsniveau heeft, zijn er twee mogelijkheden om toch gegevens naar derde landen door te mogen geven. De eerste mogelijkheid zijn de uitzonderingen die in de wet worden genoemd. Deze uitzonderingen dienen restrictief geïnterpreteerd te worden. Restrictief wil zeggen dat de wet streng moet worden geïnterpreteerd: aan de woorden van de wet wordt een minder ruime betekenis toegekend dan in het gewone spraakgebruik.

Voorbeelden van de uitzonderingen zijn de ondubbelzinnige toestemming van betrokkenen of doorgifte die noodzakelijk is in het kader van een overeenkomst bijvoorbeeld een arbeidsovereenkomst

De tweede mogelijkheid is een vergunning van de Minister van Justitie. Aan een dergelijke vergunning worden nadere voorwaarden verbonden die als waarborg voor de bescherming van persoonsgegevens dienen. Een vorm van deze waarborg is het gebruik van modelcontracten voor de doorgifte van gegevens die opgesteld worden door de Europese Commissie.

Voor de Verenigde Staten geldt een apart regime. Alleen voor die ondernemingen die zich verplicht hebben te voldoen aan de zogenaamde Veilige Haven Overeenkomst (Safe Harbor Agreement) geldt dat er sprake is van een passend beschermingsniveau. Deze lijst met ondernemingen is te vinden op de website van het U.S. Department of Commerce (www.export.gov/safeharbor).

De kwestie van de doorgifte van persoonsgegevens aan derde landen wordt verder uitgewerkt in het informatieblad "*Doorgifte naar derde landen*" en de brochure "*Derde landen*". Dit informatiemateriaal is te raadplegen op www.cbpweb.nl.

15 Worden de persoonsgegevens niet langer bewaard dan nodig?

Gegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij werden verzameld. De bewaartermijn kan meteen bij het vaststellen van het doel worden bepaald. Het is goed om met een standaardtermijn te werken, waarvan in bijzondere gevallen kan worden afgeweken.
In het zogenaamde Vrijstellingsbesluit is bepaald welke categorieÎn van verwerkingen vrijgesteld zijn van de meldingsplicht aan het College bescherming persoonsgegevens. In het Vrijstellingsbesluit staan per categorie van verwerkingen specifieke bewaartermijnen genoemd. Het is verstandig om deze termijnen toe te passen. Wijkt een bedrijf of organisatie hiervan af dan moet alsnog melding plaatsvinden van de verwerking van persoonsgegevens.

Het Vrijstellingsbesluit noemt voor personeelsadministraties een bewaartermijn van maximaal twee jaar nadat het dienstverband met de medewerker is beëindigd. Voor sollicitantenregistraties wordt een termijn genoemd van uiterlijk 4 weken nadat de sollicitatieprocedure is beëindigd.

16 Zijn voldoende maatregelen genomen om de persoonsgegevens te beveiligen?

Gegevens moeten voldoende beschermd zijn tegen onbevoegd gebruik of andere vormen van onrechtmatige verwerkingen. De ondernemer moet hiervoor zorg dragen. Het noodzakelijke niveau van beveiliging wordt bepaald aan de hand van een risicoanalyse. Hierbij zijn onder meer de aard van de gegevens en de kring van de gebruikers van belang.

Door middel van wachtwoordbeveiliging op de computer, toegangsbeveiliging of het gebruik van firewalls bij koppeling van het systeem met het internet kan bijvoorbeeld beveiliging plaatsvinden.

Het CBP-rapport *Beveiliging van persoonsgegevens* (2001) bevat een uitwerking van de wettelijke verplichting tot het beveiligen van persoonsgegevens en beveelt concrete beveiligingsmaatregelen aan (zie www.cbpweb.nl).

< VORIGE INHOUD VOLGENDE >

17 Blijft het verwerken van 'bijzondere' persoonsgegevens zoveel mogelijk achterwege?

Voor bepaalde soorten gegevens geldt een bijzonder beschermingsniveau. Het zijn gegevens die in het maatschappelijk verkeer als gevoelig worden ervaren. Het gaat om gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, en gegevens betreffende het lidmaatschap van een vakvereniging. Ook strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag zijn bijzondere gegevens.

Persoonsgegevens over iemands ras mogen alleen verwerkt worden met het oog op identificatie van de medewerker of in het kader van een voorkeursbeleid voor bepaalde minderheidsgroeperingen. Verwerking van gegevens over het lidmaatschap van een vakbond mag plaatsvinden door de vakbond zelf voor zover dat gelet op de doelstelling van de vakbond noodzakelijk is of met uitdrukkelijke toestemming van het vakbondslid.

De verwerking van deze gegevens is verboden tenzij de WBP een uitzondering geeft op dit verbod. Als de ondernemer het voornemen heeft bijzondere gegevens te verwerken, wordt aangeraden de tekst van de WBP over de bijzondere gegevens (zie artikelen 16 t/m 24) te raadplegen. Per bijzonder gegeven staan de uitzonderingen uitdrukkelijk genoemd. Daarnaast zijn er algemene uitzonderingen die voor alle bijzondere gegevens gelden.

Een voorbeeld van een algemene uitzondering is de uitdrukkelijke toestemming van de medewerker of in het geval de medewerker de persoonsgegevens zelf al duidelijk openbaar heeft gemaakt. Bijvoorbeeld als een medewerker zelf mededeelt dat hij in het verleden is veroordeeld wegens fraude en deze veroordeling van belang is voor zijn functie of voor het bedrijf.

18 Blijven medische gegevens onder beheer van een arts of van andere personen die gebonden zijn aan het medisch beroepsgeheim?

Medische gegevens zijn niet alleen bijzondere gegevens, maar vallen ook onder het medisch beroepsgeheim. Daarom is het van groot belang dat deze gegevens niet door de ondernemer worden beheerd, maar onder het beheer blijven van bijvoorbeeld de bedrijfsarts.

Medische informatie over de medewerker zal slechts met zijn uitdrukkelijke toestemming aan de ondernemer mogen worden gegeven. Een arbo-arts mag zich zonder de toestemming van de medewerker wel tegenover de ondernemer uitlaten over de vraag of deze al dan niet in staat is tot het verrichten van arbeid in het kader van reïntegratie. Ook mag de arbo-arts de ondernemer informeren over de eventuele aanpassingen op de werkplek die nodig zijn voor de reïntegratie van de medewerker. Het behoort tot de taak van de arbo-arts om de ondernemer te informeren over de beperkingen die een medewerker ondervindt ten gevolge van zijn ziekte of handicap. Het medisch beroepsgeheim geldt wel voor de gegevens die iets over de aard van de ziekte zeggen en ook bijvoorbeeld voor de uitslagen van drugs- en alcoholtests.

19 Worden de medewerkers voldoende geïnformeerd over de verwerking van hun gegevens?

Medewerkers van wie gegevens worden verwerkt, moeten kunnen nagaan wat er met die gegevens gebeurt. Volgens de WBP moet een onderneming die persoonsgegevens verwerkt, de betrokken persoon informeren over het doel van het verzamelen en de naam en het adres van het bedrijf.

De informatieplicht van de ondernemer over het verwerken van persoonsgegevens is vanzelfsprekend, wanneer de medewerker bij indiensttreding de nodige formulieren ten behoeve van de personeels- en salarisadministratie invult. Vóór het moment waarop de gegevens worden verkregen, dient dan de personeelsfunctionaris de nodige informatie te verstrekken (b.v. via een folder). Dergelijke informatie moet ook worden verstrekt bijvoorbeeld bij het ter beschikking stellen van een lease-auto. Het gaat dan om de gegevensverwerking met betrekking tot het autogebruik, zoals welke gegevens worden vastgelegd en met welk doel.

Als gegevens niet van de medewerkers worden verkregen maar van een derde, moet de medewerker worden geÔnformeerd op het moment dat de gegevens worden vastgelegd.

Een voorbeeld van gegevens die via derden worden verkregen, zijn de gegevens die bij referenties worden opgevraagd tijdens de sollicitatieprocedure. Ook moet de ondernemer de medewerker informeren wanneer hij deze observeert bij zijn gebruik van het computernetwerk of website; de medewerker verstrekt immers niet bewust deze gegevens.

20 Zijn de medewerkers op de hoogte van hun rechten en weten zij hoe zij deze kunnen uitoefenen?

Medewerkers hebben het recht op inzage in hun personeelsdossier. Ook kunnen zij verzoeken om verbetering, aanvulling, verwijdering of afscherming van hun gegevens. Hierdoor kunnen zij zich tegen onjuiste of incomplete gegevens in het dossier verweren. Op deze manier kan de medewerker voorkomen dat hij gedurende zijn gehele loopbaan door bepaalde incidenten wordt achtervolgd. Ook kunnen zij verzoeken niet meer relevante gegevens te verwijderen. Het komt ook voor dat zij na kennisneming van de gegevens behoefte hebben de eigen visie vast te leggen, bijvoorbeeld een reactie op een klacht van een klant.

Daarnaast heeft de medewerker het recht zich te verzetten tegen bepaalde verwerkingen waarbij de ondernemer een gerechtvaardigd belang heeft, maar de medewerker meent dat zijn recht op eerbiediging van de persoonlijke levenssfeer prevaleert. De ondernemer bepaalt of het verzet wordt gehonoreerd.

5

TOETSINGSVRAGEN VOOR PERSONEELS-VOLGSYSTEMEN

Bij de beoordeling van personeelsvolgsystemen kan de OR krachtens artikel 27, tweede lid onder l. van de WOR de voorgestelde regeling op de onderstaande punten toetsen.

21 Is sprake van een personeelsvolgsysteem?

Volgens de omschrijving in artikel 27, eerste lid, sub l is het instemmingsrecht van de OR van toepassing, als een voorziening gericht is op of geschikt is voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen. In het dagelijkse spraakgebruik worden dergelijke "voorzieningen" aangeduid als personeelsvolgsystemen. Als er sprake is van een personeelsvolgsysteem, dan mag er van worden uitgegaan dat er ook sprake is van verwerking van persoonsgegevens.

Vaak blijkt uit de opzet van een systeem dat het gericht is op het volgen van personeel. De wet voegt toe als criterium dat de instemming van de OR ook vereist is als een systeem daarvoor geschikt is. Er moet dus naar de mogelijke effecten van zo'n systeem worden gekeken. Als die zijn dat het personeel hoewel het in feite niet wordt gevolgd, wel kan worden gevolgd, dan is sprake van een voorziening in de zin van de WOR.

Een prikklok is gericht op controle op aanwezigheid. Een badge kan uitsluitend bedoeld zijn als een (elektronische) sleutel. Een badge kan echter ook geschikt zijn om aan- en afwezigheid van een medewerker te registreren of te observeren op welke plaats binnen een gebouw een medewerker zich bevindt. Een badge kan verder geschikt zijn voor de bediening van een koffieautomaat of als betaalmiddel in de bedrijfskantine. Ook kan een badge toegang geven tot het communicatienetwerk in het bedrijf, waarvan het in- en uitloggen van medewerkers doorgaans wordt vastgelegd.
Een videocamera is geschikt voor observatie van medewerkers. Wanneer camera's in grootwinkelbedrijven worden opgehangen uit een oogpunt van beveiliging tegen winkeldiefstal, zal een onvermijdelijk gevolg zijn dat deze ook de gedragingen van de medewerkers vastleggen. Zo kunnen de gedragingen en de prestaties van de medewerkers worden gevolgd.

Dat een voorziening ervoor geschikt is om medewerkers te observeren is niet altijd direct duidelijk. Het kan gaan om technische voorzieningen die letterlijk buiten het gezichtsveld van de medewerker liggen.

Voorzieningen die buiten het gezichtsveld van de medewerker vallen, zijn bijvoorbeeld functies van software waarmee de medewerkers dagelijks werken, zoals een programma ter voorkoming van r.s.i. Een dergelijk programma is ook geschikt om medewerkers te observeren.Ook het e-mail verkeer en internetgebruik van medewerkers is geschikt om medewerkers gade te slaan. Zo kan de ondernemer zien wanneer en aan wie de medewerker berichten verstuurt.

22 Is het nodig om gebruik te maken van een personeelsvolgsysteem?

De eerste vraag die gesteld moet worden, is of het gebruik van een personeelsvolgsysteem wel nodig is in de onderneming. Pas als deze vraag positief beantwoord wordt, komt de vraag naar de wijze van uitvoering aan de orde.

Over de noodzaak van een personeelsvolgsysteem kunnen diverse vragen worden gesteld:

a Waarom stelt de ondernemer de voorziening voor of heeft hij deze in gebruik?
b Is sprake van een wettelijke of contractuele verplichting?
c Zo niet, is het om een andere reden noodzakelijk om de voorziening in te voeren of te gebruiken?
d Als er geen van buiten komende noodzaak bestaat, kan de ondernemer dan een gerechtvaardigd belang aantonen voor het gebruik van het systeem?

< VORIGE | INHOUD | VOLGENDE >

e Hoe verhoudt zich het belang van de ondernemer tot de belangen van de medewerker? Vragen hierbij zijn
   - Hoe indringend is de observatie?
   - Komen de belangen van de medewerkers in het gedrang?
   - En zo ja, is het mogelijk om het doel dat de ondernemer voor ogen staat te bereiken op een voor de medewerkers minder belastende wijze?

Van belang is of het gebruikte middel redelijk is in verhouding tot het beoogde doel en of ook met minder ingrijpende middelen kan worden volstaan. Het is denkbaar dat de voorziening zo indringend is, dat de OR, vanuit het oogpunt van de belangen van de medewerkers en gelet op het doel dat de ondernemer voor ogen staat, niet met de regeling wil instemmen. Het is ook denkbaar dat de OR wel wil instemmen, maar onder voorwaarden. Dergelijke voorwaarden voor het gebruik van de voorziening kunnen in de regeling worden opgenomen. Enkele van die voorwaarden volgen hierna.

23 Worden de medewerkers van tevoren op de hoogte gesteld van de observatie?

De medewerkers moeten met name geïnformeerd over:
a Het doel van de observatie;
b De redenen voor observatie en tijdschema;
c Het gebruik van de verzamelde gegevens;
d Bewaartermijnen, etc.

Structureel heimelijke opnamen zijn niet toegestaan. Incidenteel kan heimelijke controle gerechtvaardigd zijn (zie onder toetsingsvraag 25). De medewerkers moeten in elk geval op het moment dat het systeem wordt ingevoerd hiervan op de hoogte worden gesteld. Verder moeten zij worden geïnformeerd over de reden van de observatie en het tijdschema dat daarbij wordt gehanteerd. Denk hierbij aan de wijze van het volgen van telefoongesprekken in call-centers. Relevante vragen zijn:
a Waarom gebeurt dit?
b Hoe vaak?
c Hoe worden medewerkers hierover en over de resultaten geïnformeerd?

24 Wordt de personeelsbeoordeling uitsluitend gebaseerd op de gegevens die met een personeelsvolgsysteem zijn verzameld?

Van belang is dat gegevens niet zomaar worden vastgelegd in de personeelsadministratie en dat niet uitsluitend op grond hiervan personeelsbeoordeling plaatsvindt. Van belang is dat medewerkers kort na de observatie door het personeelsvolgsysteem in de gelegenheid worden gesteld om te reageren op de resultaten en dat hun visie hierop bij de resultaten wordt gevoegd.

25 Is het noodzakelijk heimelijk gebruik te maken van een personeelsvolgsysteem?

Heimelijke controle (bijvoorbeeld met een verborgen camera) mag alleen in uitzonderlijke omstandigheden plaatsvinden, dus niet systematisch. Er moet sprake zijn van een redelijke verdenking ten aanzien van een of meer medewerkers die de inzet van dergelijke controle rechtvaardigt. Hierbij is vereist dat andere middelen zijn uitgeput en dat er een zwaarwegend belang van de onderneming in het geding is. In de onder- neming moet verder bekend zijn dat in uitzonderlijke situaties heimelijk een personeelsvolgsysteem kan worden ingezet.

Vragen die hierbij door de OR gesteld kunnen worden zijn:
a Staat vast welk gedrag niet wordt getolereerd?
b Zijn de betrokken medewerkers gewaarschuwd dat schadelijk gedrag niet wordt getolereerd?
c Is op een andere wijze gepoogd om het schadelijke gedrag te voorkomen of te achterhalen?
d Is dit de enige mogelijkheid die rest om het misbruik te achterhalen?
e Is voldoende gewaarborgd dat de controle niet lichtvaardig wordt ingezet?
f Wordt de betrokkene direct met de resultaten geconfronteerd?
g Krijgt hij de gelegenheid om zich te verweren?
h Wordt een beslissing tot ontslag niet louter gebaseerd op de door de controle verzamelde gegevens?
i Krijgt, afhankelijk van de ernst van hetgeen is geconstateerd, de medewerker nog een waarschuwing?

Het in het voorjaar van 2001 ingediende wetsvoorstel over uitbreiding strafbaarstelling heimelijk cameratoezicht (Kamerstukken II 2000-2001, 27 732, nr. 1-2) zal in de praktijk geen wezenlijke verandering brengen voor het camera-

< VORIGE INHOUD VOLGENDE >

toezicht op de werkvloer. Het wetsvoorstel beoogt geen verandering. Het standpunt van het CBP is dat incidenteel heimelijk cameratoezicht moet kunnen. Bij regelingen hieromtrent moet de OR betrokken worden.
Als aan de voorwaarden is voldaan dan is er geen sprake van onrechtmatigheid.

Verwerkingen van persoonsgegevens die een bijzonder risico voor de persoonlijke levenssfeer inhouden, zoals bij heimelijke observatie, worden door het CBP onderworpen aan een voorafgaand onderzoek. Het CBP onderzoekt dan de rechtmatigheid van deze gegevensverwerking. Meer informatie hierover is te vinden in het informatieblad *Voorafgaand onderzoek* op de website: www.cbpweb.nl.

BIJLAGE: OR PRIVACYCHECKLIST

Algemene toetsingsvragen	Getoetst?
1 Is sprake van een persoonsgegeven?	☐
2 Is sprake van verwerking van persoonsgegevens?	☐
3 Wie is de verantwoordelijke?	☐
4 Kan de OR gebruik maken van het instemmingsrecht?	☐
Toetsingsvragen voor de verwerking van persoonsgegevens	
5 Worden de persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt?	☐
6 Voor welk doel worden de persoonsgegevens verwerkt?	☐
7 Wanneer mogen persoonsgegevens verwerkt worden?	☐
8 Blijft het gebruik van de persoonsgegevens beperkt tot de doelen waarvoor de gegevens werden verzameld?	☐
9 Wordt volstaan met zo min mogelijk persoonsgegevens?	☐
10 Zijn voldoende maatregelen genomen om te waarborgen dat de persoonsgegevens juist en nauwkeurig zijn?	☐
11 Worden persoonsgegevens zoveel mogelijk verzameld bij de medewerker zelf?	☐
12 Hebben slechts die personen toegang tot persoonsgegevens die de gegevens nodig hebben voor de vervulling van hun taak?	☐
13 Worden gegevens ook aan personen buiten de onderneming verstrekt?	☐
14 Vindt gegevensverkeer naar het buitenland plaats?	☐
15 Worden de persoonsgegevens niet langer bewaard dan nodig?	☐
16 Zijn voldoende maatregelen genomen om de persoonsgegevens te beveiligen?	☐
17 Blijft het verwerken van ëbijzondereí persoonsgegevens zoveel mogelijk achterwege?	☐
18 Blijven medische gegevens onder beheer van een arts of van andere personen die gebonden zijn aan het medisch beroepsgeheim?	☐
19 Worden de medewerkers voldoende geÔnformeerd over de verwerking van hun gegevens?	☐
20 Zijn de medewerkers op de hoogte van hun rechten en weten zij hoe zij deze kunnen uitoefenen?	☐
Toetsingsvragen voor personeelsvolgsystemen	
21 Is sprake van een personeelsvolgsysteem?	☐
22 Is het nodig om gebruik te maken van een personeelsvolgsysteem?	☐
23 Worden de medewerkers van tevoren op de hoogte gesteld van de observatie?	☐
24 Wordt de personeelsbeoordeling niet uitsluitend gebaseerd op de gegevens die met een personeelsvolgsysteem zijn verzameld?	☐
25 Is het noodzakelijk heimelijk gebruik te maken van een personeelsvolgsysteem?	

COLLEGE BESCHERMING PERSOONSGEGEVENS

Het College bescherming persoonsgegevens (CBP) – onder de Wet bescherming persoonsgegevens (WBP) de opvolger van de Registratiekamer – houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Bij het CBP moet het gebruik van persoonsgegevens worden gemeld, tenzij hiervoor een vrijstelling geldt.

Advies, bemiddeling, onderzoek en interventie

Het CBP adviseert de regering en organisaties over de bescherming van persoonsgegevens en onderwerpen die daarmee samenhangen. Het CBP toetst gedragscodes en bemiddelt in geschillen tussen burgers en gebruikers van persoonsgegevens. Op eigen initiatief of op verzoek van een belanghebbende kan het CBP onderzoeken of de manier waarop persoonsgegevens in een bepaalde situatie zijn gebruikt, in overeenstemming is met de wet en daaraan zonodig gevolgen verbinden. Voor in gebreke blijven bij de melding kan een boete worden opgelegd. Bij overtreding van de wet of daarop gebaseerde regelingen kan het CBP overgaan tot bestuursdwang of een dwangsom opleggen.

Over zijn werkzaamheden en bevindingen brengt het CBP jaarlijks een openbaar verslag uit. Het CBP is bij de uitvoering van zijn bevoegdheden gehouden aan de normen die worden gesteld in de Algemene wet bestuursrecht. Beslissingen van het CBP zijn vatbaar voor bezwaar en beroep. Het gedrag van het CBP kan onderzocht worden door de Nationale Ombudsman.

Informatie

Voor meer informatie kunt u kijken op de website: www.cbpweb.nl.
Alle publicaties kunt u via de website bestellen of elektronisch binnenhalen; telefonisch bestellen is ook mogelijk. Voor eerste advies kunt u gebruik maken van het telefonisch spreekuur, op werkdagen van 9.00 - 12.00 uur, telefoon 070 888 85 00.

Aan de tekst van deze brochure kunnen geen rechten worden ontleend.

< VORIGE | INHOUD | VOLGENDE >