

KUNT U MIJ VOLGEN?

Een analyse van de huidige privacy regelingen
op Avans Hogeschool.

Auteur: Charelle Snoeijen
Organisatie: Avans Hogeschool
Datum: 7 januari 2014
Plaats: Tilburg

KUNT U MIJ VOLGEN?

Een analyse van de huidige privacy regelingen op
Avans Hogeschool.

Auteur:	Charelle Snoeijen
Organisatie:	Avans Hogeschool
Studentnummer:	2031199
Opleiding:	's-Hertogenbosch
Afstudeerperiode:	september 2013 - januari 2014
Classificatie:	Intern
Afstudeermentor:	Mw. mr. Y. Jurjus
Eerste afstudeerdocent:	Dhr. B.C.M. Hooijdonk
Tweede afstudeerdocent:	Dhr. B.F.M. Kratsborn
Datum:	7 januari 2014
Plaats:	Tilburg

VOORWOORD

In september 2009 ben ik gestart met de opleiding HBO Rechten aan de Juridische Hogeschool. Na een periode van hard studeren komt met deze scriptie een einde aan deze opleiding. Deze afstudeerperiode heb ik competenties als adviseren, juridisch analyseren en zelfstandige competentie verder kunnen ontwikkelen. Uiteraard heeft dit onderzoek mij tevens ervaring opgeleverd in de competentie praktijkgericht juridisch onderzoek. Dit onderzoek vergelijkt huidige regelingen op Avans Hogeschool, ter bescherming van de persoonlijke levenssfeer van werknemers, met actuele wet- en regelgeving. Het onderzoek heeft mij veel kennis gebracht over het belang van privacy en regelingen die ervoor dienen te zorgen dat de persoonlijke levenssfeer van individuen beschermd wordt. Deze scriptie is het resultaat van een vergelijkend onderzoek in opdracht van mw. mr. Y. Jurjus. Haar komt mijn dank toe voor het mogelijk maken van deze scriptie en de steun die ze mij tijdens het proces heeft verschaft. Tevens wil ik mijn dank tonen aan mw. I. Toten- van den Broek, mw. E. Uluturhan, mw. I. Kluijtmans, dhr. H. Vossen en dhr. W. Van Steen voor de informatie die ze met mij hebben gedeeld om dit onderzoek tot een goed einde te brengen. Daarnaast wil ik de docenten van de Juridische Hogeschool bedanken die mij hebben geholpen deze studie tot een succes te maken.

Rest mij u nog veel plezier toe te wensen met het lezen van deze scriptie.

Charelle Snoeijen,

Tilburg, januari 2014.

INHOUDSOPGAVE

1. Inleiding	pag. 1.
1.1. Probleembeschrijving	pag. 1.
1.2. Vraagstelling	pag. 1.
1.3. Doelstelling	pag. 1.
1.4. Deelvragen	pag. 2.
1.5. Onderzoeksstrategieën	pag. 2.
1.6. Leeswijzer	pag. 2.
2. Juridisch kader	pag. 3.
2.1. Horizontale werking	pag. 3.
2.2. Beperking van het recht op privacy	pag. 4.
2.3. Wet bescherming persoonsgegevens	pag. 6.
2.3.1. Algemene beginselen	pag. 7.
2.3.2. Rechtvaardigingsgronden	pag. 8.
2.3.3. Gevoelige gegevens	pag. 10.
2.4. Vrijstellingsbesluit	pag. 10.
2.4.1. Algemene vereisten	pag. 11.
2.4.2. Criteria voor vrijstelling	pag. 11.
2.5. Burgerlijk Wetboek	pag. 12.
2.6. Conclusie	pag. 12.
3. Huidige regelingen	pag. 13.
3.1. Internet- en e-mailgebruik	pag. 13.
3.2. Social media	pag. 16.
3.3. Cameratoezicht	pag. 18.
3.4. Telefoongebruik	pag. 20.
3.5. Nieuwe HRM systeem	pag. 21.
3.6. Conclusie	pag. 23.
4. Wat moet Avans doen om de privacy te waarborgen?	pag. 25.
4.1. Social media	pag. 25.
4.2. Telefoongebruik	pag. 26.
4.3. HRM systeem	pag. 26.
4.4. Functionaris voor de gegevensbescherming	pag. 28.
4.5. Conclusie	pag. 29.
5. Conclusies en aanbevelingen	pag. 30
5.1. Conclusies	pag. 30
5.2. Aanbevelingen	pag. 31.
6. Evaluatie onderzoek	pag. 33.

BEGRIPPENLIJST

Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder 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.

Bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

Derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.

Ontvanger: degene aan wie de persoonsgegevens worden verstrekt.

Toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

Verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens.

Verzamelen van persoonsgegevens: het verkrijgen van persoonsgegevens.

SAMENVATTING

Avans Hogeschool maakt gebruik van verscheidene reglementen die betrekking hebben op de persoonlijke levenssfeer van werknemers. In opdracht van mw. mr. Y. Jurjus worden de huidige regelingen getoetst aan actuele wet- en regelgeving. Na een analyse van de regelingen zal moeten blijken of Avans Hogeschool maatregelen dient te nemen om de bestaande regelingen in overeenstemming met de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit te brengen.

Het recht op de persoonlijke levenssfeer is vastgelegd in artikel 10 van de Grondwet en artikel 8 van het EVRM. Niet iedere inbreuk op de persoonlijke levenssfeer is onrechtmatig. Artikel 10 van de Grondwet en artikel 8 EVRM hanteren een toetsingskader om te beoordelen of sprake is van een rechtmatige inbreuk op het grondrecht. Beperken van de persoonlijke levenssfeer is mogelijk wanneer de beperking bij wet is voorzien. In Nederland is de Wet bescherming persoonsgegevens de wet die voorziet in bepalingen voor een rechtmatige inbreuk van de persoonlijke levenssfeer van burgers. Indien op basis van voornoemde wet inbreuk wordt gemaakt op de persoonlijke levenssfeer dient deze inbreuk gemeld te worden bij het College bescherming persoonsgegevens tenzij de inbreuk voldoet aan de vereisten van het Vrijstellingsbesluit.

Iedere medewerker heeft toegang tot de ICT- voorzieningen van Avans Hogeschool. In het kader van privacy is het van belang op welke manier wordt gecontroleerd op het gebruik van de ICT- faciliteiten. Het e-mail- en internetgebruik van werknemers mag op grond van de huisregels van Avans sporadisch gecontroleerd worden of bij vermoeden van misbruik. De regeling omtrent de controle op e-mail- en internetgebruik voldoet aan de vereisten van de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit. Tevens wordt er gewerkt aan een social media richtlijn. De bepalingen van die richtlijn zullen onder dezelfde regels vallen als die gelden voor het gebruik van de ICT- faciliteiten. Doordat de social media richtlijn nog niet definitief is dient na invoering van de richtlijn nader onderzocht te worden of de bepalingen voor de richtlijn in overeenstemming zijn met de wettelijke bepalingen. Het is raadzaam om voor de controle op social media aanvullende regel(s) te stellen. Het cameratoezicht is geregeld in het privacyreglement persoonsgegevens personeel. Deze regeling is momenteel nog een conceptregeling. De conceptregeling voldoet aan de wettelijke vereisten van de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit. Het is dus zaak om de conceptregeling zo spoedig mogelijk in te voeren. Avans Hogeschool ontvangt van de telefoonproviders een overzicht van alle belgegevens van de medewerkers. De mobiele telefoniegegevens worden 24 maanden bewaard. Deze bewaartermijn voldoet niet aan de vereisten van de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit. De bewaartermijn dient verlaagd te worden naar 6 maanden. Een nieuwe HRM procedure zal worden ingevoerd wanneer de privacy van de werknemers die daarmee gemoeid gaat voldoende is gewaarborgd. Om te voldoen aan de wettelijke vereisten dienen de bewaartermijnen in acht te worden genomen en medewerkeronderzoeken zullen anoniem afgenomen kunnen worden.

De huidige regelingen van Avans Hogeschool zijn niet allemaal in overeenstemming met de actuele wet- en regelgeving. De regelingen dienen te worden aangepast of er dient melding te worden gemaakt bij het College bescherming persoonsgegevens of bij een bij het College aangemelde functionaris voor de gegevensbescherming. Avans heeft een privacyfunctionaris maar deze is niet aangemeld bij het College. Avans dient de privacyfunctionaris aan te melden bij het College bescherming persoonsgegevens.

HOOFDSTUK 1

INLEIDING

In dit hoofdstuk wordt de aanleiding voor dit onderzoek beschreven. Vervolgens wordt uiteengezet op welke vraag dit onderzoek een antwoord tracht te geven. Tevens wordt omschreven wat het doel van dit onderzoek is. Tenslotte wordt omschreven met behulp van welke deelvragen en onderzoeksstrategieën tot het antwoord op de centrale vraag zal worden gekomen.

1.1. PROBLEEMBESCHRIJVING

Dit onderzoek vindt plaats bij Avans Hogeschool in opdracht van mevrouw Jurjus. Avans Hogeschool is in 2004 ontstaan door een fusie tussen Hogeschool Brabant en Hogeschool 's-Hertogenbosch. Het College van Bestuur geeft leiding aan Avans Hogeschool en de Raad van Toezicht controleert het beleid van het College van Bestuur.¹

Avans Hogeschool heeft de privacy van zowel studenten als medewerkers hoog in het vaandel staan, daarom heeft Avans twee privacyreglementen opgesteld, één voor persoonsgegevens van studenten en één voor persoonsgegevens van werknemers. Tevens zijn er verscheidene reglementen die betrekking hebben op privacy in de arbeidssfeer zoals onder andere huisregels, een privacyreglement persoonsgegevens personeel en wordt er momenteel gewerkt aan een social media protocol

Er zijn dus verscheidene reglementen waarin het aspect privacy naar voren komt maar er is geen allesomvattend beleid. Tevens is onlangs een nieuwe HR procedure opgestart wat voornamelijk digitalisering van verscheidene documenten inhoudt. Een geheel nieuwe werkwijze, die hoofdzakelijk neerkomt op digitalisering, maakt dat regelingen zoals het privacyreglement dienen te worden toegespitst op deze nieuwe methode van werken en andersom dient de nieuwe werkwijze te worden getoetst op privacy aspecten. Om de persoonlijke levenssfeer van medewerkers te waarborgen is een duidelijk uitgekristalliseerd privacy beleid wenselijk. Om een dergelijk privacy beleid te realiseren worden in opdracht van Avans Hogeschool de bestaande regelingen die privacy aspecten in zich bergen getoetst aan geldende en relevante wetgeving en actuele jurisprudentie op het gebied van privacy. Na een analyse zal moeten blijken of de huidige regelingen op het gebied van privacy in de arbeidssfeer van Avans Hogeschool correct en adequaat wordt toegepast of dat nader beleid dient te worden ontwikkeld.

1.2. VRAAGSTELLING

Welke maatregelen dient Avans Hogeschool te nemen om bestaande interne regelingen die privacy aspecten bevatten overeen te laten stemmen met de Wet bescherming persoonsgegevens en het vrijstellingsbesluit?

1.3. DOELSTELLING

Op 6 januari 2013 wordt een adviesrapport overhandigd aan het College van Bestuur van Avans Hogeschool waarin aanbevelingen staan om huidige privacy regelingen in

¹ Organisatie Avans Hogeschool', www.avans.nl, (zoek op: organisatie).

overeenstemming te brengen met de Wet bescherming persoonsgegevens en het vrijstellingsbesluit. De aanbevelingen zijn gebaseerd op een vergelijking van bestaande privacyregelingen van Avans Hogeschool met de Wet bescherming persoonsgegevens en het vrijstellingsbesluit.

1.4. DEELVRAGEN

Aan de hand van de volgende deelvragen wordt getracht tot een antwoord op de centrale vraag te komen.

- 1) Wat is het juridisch kader?
- 2) Welke privacy aspecten komen aan bod in de huidige regelingen van Avans Hogeschool?
- 3) Welke verschillen zijn er met de huidige privacyregelingen en de Wet bescherming persoonsgegevens en het vrijstellingsbesluit?
- 4) Wat moet Avans Hogeschool doen om de privacy in de huidige regelingen te waarborgen?

1.5. ONDERZOEKSSTRATEGIEËN

Voor het onderzoek van relevante wet- en regelgeving op het gebied van privacy in de arbeidssfeer zal een rechtsbronnen- en literatuuronderzoek worden verricht. De rechtsbronnen en literatuur worden geanalyseerd, vergeleken met het huidige privacy beleid en vervolgens geïnterpreteerd. De aard van het onderzoek is kwalitatief waarbij als strategie 'casestudy' van toepassing is. Er is sprake van een enkelvoudige casestudy waarbij gebruik wordt gemaakt van verschillende onderzoeksmethoden. De onderzoeksmethoden die in dit onderzoek aan bod komen zijn een inhoudsanalyse en interview. Een inhoudsanalyse is een methode waarbij gebruik wordt gemaakt van bestaand materiaal. In dit geval zal het materiaal bestaan uit wetten, verdragen jurisprudentie, vakliteratuur, documenten en materiaal afkomstig van internet en databanken.² De bestaande documenten zullen vergeleken worden met de huidige privacy regelingen van Avans Hogeschool. Tevens wordt gebruik gemaakt van de methode interview. Met behulp van interviews wordt achterhaald of de huidige praktijk werkt of dat medewerkers tegen problemen aanlopen met betrekking tot de huidige regelingen omtrent privacy. Tevens dient het nieuwe HRM proces middels interviews onderzocht te worden om te bepalen of de nieuwe methode moeilijkheden met zich meebrengt omtrent de privacy van medewerkers. De interviews die worden afgenomen zijn half gestructureerd. Bij een half gestructureerd interview is sprake van een vragenlijst of een lijst met onderwerpen maar er is ook alle ruimte voor eigen inbreng van de geïnterviewde.³

1.6. LEESWIJZER

Dit document bestaat uit zes hoofdstukken. Na de inleiding schetst hoofdstuk twee het juridisch kader. In hoofdstuk drie worden de huidige regelingen van Avans uiteengezet en getoetst aan de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit. Vervolgens beschrijft hoofdstuk vier wat Avans moet doen om de bestaande regelingen in

² G.A.F.M. Schaaik, Praktijkgericht juridisch onderzoek, Den Haag: Boom juridische uitgevers 2011.

³ G.A.F.M. Schaaik, Praktijkgericht juridisch onderzoek, Den Haag: Boom juridische uitgevers 2011.

overeenstemming met de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit te brengen. Hoofdstuk vijf bevat de conclusies en aanbevelingen op basis van de onderzoeksresultaten. Tot slot wordt in hoofdstuk zes het verloop van dit onderzoek geevalueerd.

HOOFDSTUK 2

JURIDISCH KADER

In dit hoofdstuk ligt het accent op het juridisch kader rondom privacy. Er wordt een juridisch kader geschetst om de geldigheid van de huidige regelingen op Avans Hogeschool te kunnen beoordelen. Allereerst wordt een korte introductie over grondrechten en het begrip 'persoonlijke levenssfeer' gegeven. Vervolgens wordt beschreven onder welke voorwaarden het recht op privacy beperkt mag worden. Voorts worden de Wet bescherming persoonsgegevens, de Europese richtlijn inzake privacy en het vrijstellingsbesluit behandeld. Tenslotte worden de relevante bepalingen uit het Burgerlijk Wetboek besproken.

2.1 HORIZONTALE WERKING VAN HET RECHT OP PRIVACY

Uit artikel 10 lid 1 van de Grondwet, artikel 8 EVRM en artikel 17 IVBPR valt niet op te maken wat onder het begrip 'persoonlijke levenssfeer' begrepen moet worden. Het begrip privacy wordt vaak aangeduid als het recht om zijn eigen leven te leiden met zo min mogelijk inmenging van buitenaf.⁴ Uit jurisprudentie en literatuur valt meer specifiek op te maken dat tot de persoonlijke levenssfeer in ieder geval zijn te rekenen: de woning, bepaalde vormen van communicatie, vertrouwelijke gesprekken, sommige individuele gewoonten, gedragingen, contacten, abonnementen, lidmaatschappen e.d., bepaalde aspecten van het gezinsleven, lichamelijke en geestelijke integriteit en de verwerking van persoonsgegevens.⁵

Er wordt onderscheid gemaakt tussen de horizontale en verticale werking van grondrechten. Met horizontale werking wordt de rechtsbetrekking tussen burgers onderling bedoeld. Artikel 8 EVRM behelst een positieve verplichting (het effectiviteitsprincipe) richting de overheid welke eruit kan bestaan, dat de staat een individu moet beschermen tegen inbreuk van zijn recht op privacy door een ander individu. Het is algemeen aanvaard dat niet alleen de overheid geen inbreuken op de persoonlijke levenssfeer (privacy) mag maken, maar ook de ene burger niet ten opzichte van de ander.⁶ Er wordt dan gesproken van een directe of indirecte horizontale werking van grondrechten.

Uit een arrest⁷ van de Hoge Raad van 9 januari 1987 blijkt dat het grondrecht privacy van artikel 8 EVRM horizontale werking heeft. In bovengenoemd arrest heeft verweerder gedurende een zekere tijd informatie over het privéleven van eiseres verzameld. In het onderhavige geval was de verweerder de buurman van eiseres waarbij noemenswaardig is dat de buurman als adjunct-directeur van de GSD van Edam-Volendam werkzaam was. Mede naar aanleiding van de aldus vergaarde informatie werd besloten de aan eiseres toegekende bijstandsuitkering te beëindigen. De gedragingen van de verweerder leveren een inbreuk op het recht van de eiseres op eerbiediging van haar persoonlijke levenssfeer op. De Hoge Raad erkend in het arrest dat het recht op eerbiediging van de persoonlijke levenssfeer (artikel 8 EVRM) ook werking heeft tussen burgers onderling.

Grondrechten worden door de Hoge Raad, vaker dan voorheen, nadrukkelijk relevant

⁴I. van der Helm, 'De privacybescherming van de zieke werknemer', Deventer: Kluwer, 2009.

⁵G. Overkleef-Verburg, 'De Grondwet, een systematisch en artikelsgewijs commentaar', Deventer, 2000.

⁶D.J. Elzinga en R. De Lange, 'Het handboek van het Nederlandse staatsrecht', Deventer: Kluwer, 2006.

⁷HR 9 januari 1987, LJN: AG5500.

geacht in privaatrechtelijke relaties.⁸ Zeker als de ene burger ten opzichte van de ander in een machtige positie verkeert, is het belang van horizontale werking aanzienlijk. Dit is ook het geval met de positie van werkgever en werknemer. Een werkgever heeft ten opzichte van de werknemer een machtige positie.

Het oordeel dat de rechten van het individu zijn geschonden houdt tegelijk het oordeel in dat de staat tekort geschoten is in zijn plicht die rechten te beschermen.⁹ Dit wordt ook wel het effectiviteitsprincipe genoemd. De Staat moet ervoor zorgen dat de burger niet het slachtoffer wordt van bijvoorbeeld schending van het recht op privacy. Die bescherming wordt in dit geval vooral geboden middels de Wet bescherming persoonsgegevens.

2.2 BEPERKING VAN HET RECHT OP PRIVACY

Artikel 10 van de Grondwet en artikel 8 EVRM beschermen tegen willekeurige inbreuken op de privacy.¹⁰ Beide artikelen bevatten een beperkingsclausule. Wanneer aan de voorwaarden voor beperking van het grondrecht privacy is voldaan, wordt gesproken van een rechtmatige inbreuk op de privacy. Indien niet aan de voorwaarden is voldaan is sprake van schending van het recht op privacy.

De grondwet hanteert een formeel toetsingscriterium om te bepalen of een inbreuk op de privacy gerechtvaardigd is. Het toetsingscriterium luidt: een beperking op de persoonlijke levenssfeer en de lichamelijke integriteit is toegestaan indien de beperking 'bij of krachtens de wet' is geregeld. Onder 'wet' dient wet in formele zin te worden verstaan. Een beperking van het recht op de persoonlijke levenssfeer is dus alleen gerechtvaardigd indien die beperking een grondslag heeft in een wet in formele zin.¹¹ In bepaalde gevallen is delegatie aan een lagere regelgever mogelijk.¹²

Artikel 8 EVRM heeft een breder toetsingskader. In eerste instantie dient te worden beoordeeld of er daadwerkelijk sprake is van een inbreuk op de privacy. Wanneer dit inderdaad zo blijkt te zijn wordt vervolgens onderzocht of sprake is van een gerechtvaardigde inbreuk. Artikel 8 lid 2 EVRM noemt hiervoor 3 voorwaarden. Een inbreuk op de privacy is gerechtvaardigd als deze inbreuk '*in accordance with the law*' is, die inbreuk een '*legitimate aim*' dient, en die inbreuk '*neccessary in a democratic society*' is.

'*In accordance with the law*' is de eerste voorwaarde van artikel 8 lid 2 EVRM. In de Nederlandse vertaling van het EVRM wordt deze term aangeduid met: 'bij de wet voorzien'. Deze voorwaarde kent twee aspecten. De eerste is dat de inbreuk op de privacy volgens het nationale recht geoorloofd moet zijn. Uit deze bepaling vloeit voort dat, indien sprake is van schending van het nationale recht, dit per definitie een schending van het verdrag oplevert. Het tweede aspect behelst de kwaliteit van het nationale recht. De meeste grondrechten behoeven nadere wettelijke precisering met betrekking tot

⁸HR 8 oktober 2004, nr. C03/077HR. In dit arrest erkent de Hoge Raad de horizontale werking van artikel 1 van de Grondwet. In deze zaak betreft het de vraag of de cao voor vliegers *Martinair Holland N.V.*, in strijd is met het verbod van discriminatie als bedoeld in artikel 1 Grondwet en artikel 26 IVBPR. De cao hield in dat de arbeidsovereenkomst van de vlieger bij 56- of 58 jarige leeftijd van de vlieger eindigt, zonder dat daartoe opzegging is vereist.

⁹B.F. Keulen en G. Knigge, 'Kennismaking met het EVRM', Deventer: Kluwer, 2012, p. 65 -104.

¹⁰B.F. Keulen en G. Knigge, 'Kennismaking met het EVRM', Deventer: Kluwer, 2012, p. 65 -104.

¹¹I. van der Helm, 'De privacybescherming van de zieke werknemer', Deventer: Kluwer, 2009.

¹²Commissie Grondrechten in het digitale tijdperk, Rotterdam: Phoenix en Den Oudsten, 2000.

beperkingen en toepassing.¹³ In beginsel kunnen alleen door de overheid opgestelde regels voor de uitoefening van publiekrechtelijke bevoegdheden aangemerkt worden als 'recht' (*law*). Indien een regeling volgt uit bijvoorbeeld een arbeidsovereenkomst dan is die regeling niet aan te merken als 'recht'. De schriftelijke voorschriften van de werkgever kunnen niet dienen als een rechtsgrondslag voor een beperking aangezien deze niet als 'recht' kunnen worden aangemerkt. Indien de beperking van het recht op privacy hoofdzakelijk voortvloeit uit een regeling van de werkgever die de status van recht ontbeert, betekent dit niet dat de beperking geen grondslag in het nationale 'recht' heeft. De regel op grond waarvan de inbreuk plaatsvindt hoeft slechts een basis in het nationale recht te hebben, de regeling hoeft dus niet specifiek in het nationale recht geregeld te zijn maar de regeling dient dan wel tot een wetsebepaling te herleiden.¹⁴

De '*rule of law*' beoogt willekeur tegen te gaan. De wettelijke bepaling mag daarom niet vaag en onbepaald zijn. Om onder het begrip '*law*' te vallen dient te worden voldaan aan de eisen van toegankelijkheid (*accessibility*) en voorzienbaarheid (*foreseeability*) tevens moet de regel voldoende specifiek zijn geformuleerd, m.a.w. de regels moeten rechtszekerheid bieden. Regels die behoorlijk zijn gepubliceerd zoals publicatie in het Staatsblad en de Staatscourant worden toegankelijk geacht. De voorzienbaarheid houdt in dat de wettelijke regeling met voldoende precisie is geformuleerd zodat de burger op de hoogte is van wat de inbreuken op zijn recht op privacy kunnen zijn. De burger moet, eventueel met behulp van advies, de consequenties van een bepaald handelen kennen zodat hij zijn gedrag daar op af kan stemmen.¹⁵ Hoe groter de inbreuk is die op de privacy wordt gemaakt, hoe nauwkeuriger de wettelijke regeling dient te zijn en hoe stringenter de voorwaarden die daarbij worden gesteld.¹⁶ Om het recht op privacy te mogen beperken is nadere wettelijke precisering nodig. Een voorbeeld van zulke wettelijke precisering is de Wet Bescherming Persoonsgegevens. De Wet Bescherming Persoonsgegevens wordt later in dit hoofdstuk nog uitvoerig behandeld.

De tweede voorwaarde die artikel 8 lid 2 EVRM noemt is of de inbreuk een '*legitimate aim*' dient. Oftewel de inbreuk moet een legitiem doel dienen. De doelcriteria genoemd in artikel 8 lid 2 EVRM kunnen een grond zijn voor de beperking van het recht op privacy. De inbreuk moet in het belang zijn van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Het laatste doelcriterium: voor de bescherming van de rechten en vrijheden van anderen is in het kader van dit onderzoek van belang. De belangen van een werkgever kunnen bij de uitvoering van de regeling een grond zijn om het recht op privacy van de werknemer te beperken.¹⁷ Het Hof maakt geen onderscheid tussen rechten en belangen zo blijkt uit jurisprudentie.¹⁸ Belangen vallen onder het begrip 'rechten van anderen'.¹⁹ Rechtens te respecteren belangen van een ander kunnen daarom een gerechtvaardigde reden zijn om het recht op privacy te beperken. De ruime interpretatie van deze beperkingsgrond is nodig voor de toepassing ervan in horizontale

¹³ D.J. Elzinga en R. De Lange, 'Het handboek van het Nederlandse staatsrecht', Deventer: Kluwer, 2006, p. 289.

¹⁴ I. van der Helm, 'De privacybescherming van de zieke werknemer', Deventer: Kluwer, 2009.

¹⁵ I. van der Helm, 'De privacybescherming van de zieke werknemer', Deventer: Kluwer, 2009.

¹⁶ B.F. Keulen en G. Knigge, 'Kennismaking met het EVRM', Deventer: Kluwer, 2010.

¹⁷ I. van der Helm, 'De privacybescherming van de zieke werknemer', Deventer: Kluwer, 2009.

¹⁸ ERHM 25 maart 1985, nr. NJ 1987,900 (Barthold/ Bondsrepubliek Duitsland).

¹⁹ EHRM 7 juli 1989, nr. NJ1991,659 (Gaskin/ Verenigd Koninkrijk).

verhoudingen.

Tenslotte word als laatste voorwaarde '*neccessary in a democratic society*' genoemd. Het gaat om de vraag of de inbreuk noodzakelijk is in een democratische samenleving. Dit moet worden beoordeeld met behulp van de proportionaliteitstoets waarmee antwoord wordt gegeven op de vraag of de gemaakte inbreuk in verhouding staat tot het nagestreefde doel. Tevens dient te worden beoordeeld of een middel is gebruikt dat de minste inbreuk maakt op de privacy. Dit wordt het beginsel van subsidiariteit genoemd. Dit beginsel ziet er op toe of het beoogde doel van de inbreuk met een minder ingrijpend middel kan plaatsvinden. De proportionaliteit ziet toe op de beoordeling of er evenredigheid is tussen het doel en het middel.²⁰

2.3 WET BESCHERMING PERSOONSgegevens

Artikel 10 eerste lid van de Grondwet behelst, zoals eerder in dit hoofdstuk is aangegeven, het recht op eerbiediging van de persoonlijke levenssfeer. Het tweede en derde lid stellen dat de wetgever nadere maatregelen dient te treffen over het omgaan met persoonsgegevens. Hieraan is invulling gegeven door voorheen de Wet persoonsregistraties en nu als opvolger van die wet de Wet bescherming persoonsgegevens. Ook op grond van de EU-richtlijn²¹ betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, dienden alle lidstaten implementatiewetgeving tot stand te brengen. De richtlijn heeft als voornaamste doel dat de lidstaten dezelfde norm hanteren ter bescherming van persoonsgegevens. Zodoende is op 1 september 2001 de Wet bescherming persoonsgegevens in werking getreden.

Het hoofdthema van de Wet bescherming persoonsgegevens is het verwerken²² van persoonsgegevens.²³ Diverse vormen van het verwerken van persoonsgegevens zoals cameratoezicht, dienen rechtstreeks getoetst te worden aan de wettelijke normen van de Wet bescherming persoonsgegevens.²⁴ Er is als sprake van het verwerken van persoonsgegevens als deze gegevens mondeling of schriftelijk worden gevraagd. Het is daarbij niet relevant of de betrokkene wel of niet gehoor geeft aan het verzoek om persoonsgegevens.²⁵

Artikel 2 lid 1 van de Wet bescherming persoonsgegevens stelt dat deze wet van toepassing is op geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand²⁶ zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. In beginsel geldt dat de Wet bescherming persoonsgegevens van toepassing is tenzij er sprake is van de gevallen genoemd in die wet.

Het tweede lid van datzelfde artikel noemt bepaalde gevallen waarbij de Wet bescherming persoonsgegevens niet van toepassing is.

²⁰ I. van der Helm, 'De privacybescherming van de zieke werknemer', Deventer: Kluwer, 2009.

²¹ Richtlijn 95/46/EG (PbEG 1995 L 281/31).

²² Zie voor de definitie van 'verwerken' de begrippenlijst.

²³ Zie voor de definitie van 'persoonsgegevens' de begrippenlijst.

²⁴ H.H. De Vries en D.J. Rutgers, 'Wet bescherming persoonsgegevens toepassing in arbeidsverhoudingen', Deventer: Kluwer, 2001.

²⁵ Kamerstukken II 1997/1998, 25892, nr. 3, (MvT).

²⁶ Zie voor de definitie van 'bestand' de begrippenlijst.

De Wet bescherming persoonsgegevens is op grond van artikel 2 lid 2 juncto. Artikel 3 lid 1 van die wet niet van toepassing wanneer persoonsgegevens worden verwerkt:

- 5) ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden. Op de werkvloer is hier bijvoorbeeld sprake van wanneer een werknemer zelf een lijst bijhoudt met adressen van contactpersonen.²⁷
- 6) door of ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten;
- 7) ten behoeve van de uitvoering van de politietaak, omschreven in artikel 2 van de politiewet 1993;
- 8) die is geregeld bij of krachtens de Wet gemeentelijke basisadministratie persoonsgegevens;
- 9) ten behoeve van de uitvoering van de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag, en;
- 10) ten behoeve van de uitvoering van de Kieswet;
- 11) voor uitsluitend journalistieke, artistieke of literaire doeleinden.²⁸

2.3.1. ALGEMENE BEGINSELEN VAN GEGEVENSVERWERKING

Artikel 6 van de Wet bescherming persoonsgegevens bevat een algemeen basisprincipe over het verwerken van persoonsgegevens. Het artikel bepaald dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze dienen te worden verwerkt. Hierop aansluitend wordt in artikel 7 van de Wet bescherming persoonsgegevens bepaald dat persoonsgegevens alleen voor welbepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. Artikel 7 en artikel 9 van de Wet bescherming persoonsgegevens vormen samen het 'doelbindingsprincipe'. Artikel 9 bepaald namelijk dat persoonsgegevens niet nader mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Artikel 9 biedt, bij de afweging of de gegevensverwerking verenigbaar is met de doeleinden waarvoor ze zijn verkregen, een handvat waarin factoren worden genoemd waar de verantwoordelijke²⁹ in ieder geval rekening mee dient te houden. Tevens worden andere factoren in de wet genoemd die bij de afweging als mede een rol kunnen spelen.³⁰ Ter handhaving van de Wet bescherming persoonsgegevens stelt deze wet het College bescherming persoonsgegevens in als toezichthouder.

Aan de verantwoordelijke komen een aantal verplichtingen toe die voortvloeien uit de Wet bescherming persoonsgegevens:

Meldingsplicht:

De verantwoordelijke dient, conform artikel 27 van die wet, voordat hij begint met het verwerken van persoonsgegevens die verwerking te melden bij het College bescherming persoonsgegevens of bij de functionaris voor de gegevensbescherming. Het overtreden van de meldingsplicht wordt op grond van artikel 75 Wet bescherming persoonsgegevens aangemerkt als een strafbaar feit. De meldingsplicht heeft als doel de verantwoordelijke³¹ te stimuleren om zich te verantwoorden voor welke doeleinden hij persoonsgegevens wilt

²⁷ H.H. De Vries en D.J. Rutgers, 'Wet bescherming persoonsgegevens, toepassing in arbeidsverhoudingen', Deventer: Kluwer, 2001.

²⁸ Kamerstukken II 1997/1998, 25892, nr. 3, (MvT).

²⁹ Zie voor de definitie van 'verantwoordelijke' de begrippenlijst.

³⁰ Kamerstukken II 1997/1998, 25892, nr. 3, (MvT).

³¹ Zie voor de definitie van 'verantwoordelijke' de begrippenlijst.

verzamelen en waarom die verzameling van persoonsgegevens noodzakelijk is voor dat doel.

Bepaalde gegevensverwerkingen worden vrijgesteld van de meldingsplicht. Voor meer informatie over de vrijstelling zie paragraaf 2.5.

Bewaartermijn:

Ingevolge artikel 10 Wet bescherming persoonsgegevens mogen de persoonsgegevens niet langer worden bewaard dan noodzakelijk voor het verwezenlijken van de doeleinden waarvoor de gegevens verzameld en/of verwerkt worden.

Beveiliging:

De verantwoordelijke dient op grond van artikel 13 Wet bescherming persoonsgegevens passende technische en organisatorische maatregelen te treffen tegen enige vorm van onrechtmatige verwerking.

Transparantiebeginsel:

Het transparantiebeginsel houdt in dat het voor de betrokkene helder moet zijn wat er met zijn persoonsgegevens gebeurt. Het is voor betrokkene van belang dat hij op de hoogte wordt gesteld van de verwerking van gegevens die op hem betrekking hebben zodat hij in staat is zijn rechten te verwezenlijken. Doordat de kans omwille van de nieuwe communicatietechnieken groter is dat er persoonsgegevens worden verwerkt buiten medeweten van de betrokkene om, is de verplichting van de verantwoordelijke op transparantie in de Wet bescherming persoonsgegevens aangescherpt. De informatieplicht is geregeld in de artikelen 33 en 34 van de Wet bescherming persoonsgegevens.

Schadevergoeding:

De verantwoordelijke is op grond van artikel 49 lid 1 Wet bescherming persoonsgegevens aansprakelijk wanneer iemand schade lijdt als gevolg van het overtreden van de Wet bescherming persoonsgegevens. De verantwoordelijke is voor zowel materiële als immateriële schade aansprakelijk.

Naast het feit dat er aan de verantwoordelijke verplichtingen toekomen, komen aan de betrokkene rechten toe:

Recht op inzage:

In artikel 35 van de Wet bescherming persoonsgegevens is geregeld dat de betrokkene zich tot de verantwoordelijke kan wenden met het verzoek hem mede te delen of er persoonsgegevens van hem verwerkt worden. De verantwoordelijke dient binnen vier weken na het verzoek schriftelijk te antwoorden op het verzoek van de betrokkene.

Recht op correctie:

Indien de persoonsgegevens van betrokkene feitelijk onjuist zijn, onvolledig of niet ter zake dienend voor het doel waarvoor ze zijn verwerkt of in strijd is met een wettelijk voorschrift kan de betrokkene ingevolge artikel 36 van de Wet bescherming persoonsgegevens de verantwoordelijke verzoeken om correctie van de gegevens. Een correctie kan eruit bestaan dat de verantwoordelijke de gegevens verbeterd, aanvult, verwijderd of afschermt.

Recht van verzet:

De betrokkene kan zich op grond van artikel 40 Wet bescherming persoonsgegevens tegen bepaalde gegevensverwerking verzetten. Het gaat dan in beginsel om een rechtmatige gegevensverwerking, maar deze wordt onrechtmatig wanneer het verzet is aangetekend en

het verzet gegrond word geacht. Verzet is mogelijk tegen de werkingsgrond van artikel 8 sub e en f van de Wet bescherming persoonsgegevens.

2.3.2. RECHTVAARDIGINGSGRONDEN VOOR GEGEVENSVERWERKING

Het criterium 'gerechtvaardigde doeleinden' uit artikel 7 van de Wet bescherming persoonsgegevens vindt nadere uitwerking in artikel 8 van de Wet bescherming persoonsgegevens. In deze bepaling worden limitatief de gronden opgesomd voor het rechtvaardigen van de verwerking van persoonsgegevens. Iedere verwerking van persoonsgegevens dient minstens op één van de in artikel 8 genoemde rechtvaardigingsgronden te berusten:

Ondubbelzinnige toestemming van de betrokkene:

Toestemming van de betrokkene wordt in artikel 1 sub i omschreven als: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanaardt dat hem betreffende persoonsgegevens worden verwerkt.

Om te bepalen of er daadwerkelijk toestemming is verkregen dient aan drie criteria te zijn voldaan:

- 1) De betrokkene³² dient zijn toestemming in vrijheid te hebben geuit. Indien sprake is van enige druk die geleid heeft tot het geven van de toestemming dan dient te worden aangenomen dat de betrokkene geen toestemming heeft verleend.
- 2) De toestemming van de betrokkene moet betrekking hebben op specifieke gegevensverwerkingen of een beperkte categorie gegevensverwerkingen.
- 3) De betrokkene dient zo goed mogelijk geïnformeerd te worden over de gegevensverwerking zodat de betrokkene weloverwogen toestemming kan geven.

Tevens dient de toestemming ondubbelzinnig te zijn. Ondubbelzinnig wil zeggen dat elk twijfel bij de verantwoordelijke dient te zijn uitgesloten over de vraag of de betrokkene zijn (mondelinge of schriftelijke) toestemming heeft gegeven en voor welke specifieke gegevensverwerking deze toestemming is gegeven. Indien er twijfel bestaat over de vraag of betrokkene zijn toestemming heeft verleend, dient de verantwoordelijke te bewijzen dat betrokkene toestemming heeft gegeven voor de gegevensverwerking. Conform artikel 5 lid 2 van de Wet bescherming persoonsgegevens kan de betrokkene de eenmaal gegeven toestemming te allen tijde intrekken.

In geval de toestemming niet aan bovengenoemde criteria voldoet is deze nietig. Omdat het recht op eerbiediging van de persoonlijke levenssfeer een zaak van openbare orde is, is artikel 3:40 lid 1 BW van toepassing. Dit artikel bepaalt dat wanneer een rechtshandeling die door zijn inhoud of strekking in strijd is met de openbare orde of de goede zeden, de rechtshandeling nietig is.³³

De gegevensverwerking is noodzakelijk om contractuele verplichtingen na te komen:

Voorwaarde bij deze rechtvaardigingsgrond is dat de betrokkene partij is bij de desbetreffende overeenkomst of een precontractuele fase. Het is daarbij niet noodzakelijk dat de verantwoordelijke zelf betrokken is bij de overeenkomst. Voorts hoeft de bedoelde overeenkomst niet specifiek gericht te zijn op de verwerking van persoonsgegevens, maar de gegevensverwerking kan een noodzakelijk uitvloeisel zijn van de overeenkomst. Dit is bijvoorbeeld het geval bij de verwerking van salarisgegevens als uitvloeisel van de

³² Zie voor de definitie van 'betrokkene' de begrippenlijst.

³³ *Kamerstukken II 1997/1998, 25892, nr. 3, p. 67 (MvT).*

arbeidsovereenkomst.³⁴ Wanneer het gaat over de precontractuele fase is gegevensverwerking geoorloofd als het gaat om handelingen die op verzoek van de betrokkene worden verricht met als doel een overeenkomst te kunnen sluiten. Hierbij is van belang dat de handelingen voortvloeien uit het verzoeken dat betrokkene redelijkerwijs kon verwachten dat die handelingen werden verricht.

Nakomen van een wettelijke verplichting:

Het is de verantwoordelijke toegestaan gegevens te verwerken wanneer dit noodzakelijk is ter uitvoering van een wettelijke verplichting die op hem rust. De wettelijke verplichting dient op de verantwoordelijke zelf te rusten en dient noodzakelijkerwijs met zich mee te brengen dat de desbetreffende gegevens worden verwerkt.

Bestrijding van ernstig gevaar voor de gezondheid van de betrokkene:

De privacy richtlijn³⁵ spreekt van een geoorloofde verwerking wanneer de verwerking wordt uitgevoerd ter bescherming van een belang dat voor het leven van de betrokkene essentieel is. De formulering uit de Wet bescherming persoonsgegevens moet ook in dat licht worden geïnterpreteerd. Het verwerken van de gegevens van betrokkene is gerechtvaardigd wanneer het gaat om een zaak van leven of dood.

Goed vervulling van een publiekrechtelijke taak:

Gegevensverwerking is mogelijk voor zover deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het betreffende bestuursorgaan dan wel het bestuursorgaan aan wie de gegevens worden verstrekt.³⁶ Het gaat hierbij om taken die specifiek bij een bestuursorgaan worden neergelegd en niet om taken die ook door particulieren worden verricht. Het sluiten van een arbeidsovereenkomst door een bestuursorgaan kan daarom ook niet gebaseerd worden op deze rechtvaardigingsgrond.

Behartiging van een gerechtvaardigd belang:

De gegevensverwerking is conform onderdeel f van artikel 8 van de Wet bescherming persoonsgegevens gerechtvaardigd wanneer deze verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, doorslaggevend zijn.³⁷ Een gerechtvaardigd belang wordt bijvoorbeeld aanwezig geacht wanneer de gegevensverwerking noodzakelijk is om reguliere bedrijfsactiviteiten te kunnen verrichten.³⁸

Om te bepalen of er sprake is van een gerechtvaardigd belang beschrijft de Memorie van Toelichting bij de Wet bescherming persoonsgegevens een aantal vragen welke de verantwoordelijke voor zichzelf dient te beantwoorden:

- 1) Is er werkelijk een belang dat verwerking van persoonsgegevens rechtvaardigt?

³⁴ H.H. De Vries en D.J. Rutgers, 'Wet bescherming persoonsgegevens, toepassing in arbeidsverhoudingen', Deventer: Kluwer, 2001.

³⁵ Richtlijn 95/46/EG (PbEG 1995 L 281/31).

³⁶ Kamerstukken II 1997/1998, 25892, nr. 3, p. 85 (MvT).

³⁷ Kamerstukken II 1997/1998, 25892, nr. 3, p. 86 (MvT).

³⁸ H.H. De Vries en D.J. Rutgers, 'Wet bescherming persoonsgegevens, toepassing in arbeidsverhoudingen', Deventer: Kluwer, 2001.

- 2) Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan – afhankelijk van de ernst van de inbreuk – gegevensverwerking niet achterwege te blijven?
- 3) Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg – zonder verwerking – worden bereikt? (subsidiariteit)
- 4) Is de verwerking in de mate die is beoogd evenredig aan het nagestreefde doel? (proportioneel)³⁹

2.3.3. VERWERKING VAN GEVOELIGE PERSOONSgegevens

Iedere vorm van gegevensverwerking behoeft een rechtvaardiging als bedoeld in artikel 8 van de Wet bescherming persoonsgegevens. Wanneer sprake is van gevoelige persoonsgegevens zoals: gezondheid, ras, politieke gezindheid, seksueel leven, strafrechtelijke persoonsgegevens en het lidmaatschap van een vakvereniging. De verwerking van deze gegevens is in beginsel niet toegestaan, maar er zijn een aantal uitzonderingen. Deze uitzonderingen vinden grondslag in paragraaf 2 van hoofdstuk 2 van de Wet bescherming persoonsgegevens⁴⁰ Ingevolge artikel 23 lid 1 onder e Wet bescherming persoonsgegevens is de belangrijkste algemene garantie dat de verwerking van gevoelige gegevens niet is toegestaan dan voor zover dat bij wet is bepaald.

2.4. VRIJSTELLINGSBESLUIT

Zoals eerder in dit hoofdstuk is opgemerkt komen bepaalde vormen van gegevensverwerking in aanmerking voor een vrijstelling van de meldingsplicht. Het niet-nakomen van de meldingsplicht kan tot een boete leiden voor de verantwoordelijke. Vrijstelling van de meldplicht is mogelijk als blijkt dat een inbreuk op de rechten en vrijheden van de betrokkenen door de verwerkingen onwaarschijnlijk is. Uitgangspunt hierbij is dat de inbreuk op de persoonlijke levenssfeer onwaarschijnlijk is bij gegevensverwerkingen die standaard zijn en waarvan in het algemeen bekend is dat deze voorkomen.⁴¹ Als een gegevensverwerking is vrijgesteld van de meldplicht dient de gegevensverwerking verder in overeenstemming te zijn met de overige eisen die de Wet bescherming persoonsgegevens stelt aan de verwerking van persoonsgegevens.

Er geldt een algehele vrijstelling voor verwerkingen betreffende openbare registers die bij de wet zijn ingesteld. Het gaat hierbij om registers die een grondslag in de formele wet hebben en voor iedereen vrij toegankelijk zijn.⁴² Tevens geldt er een algehele vrijstelling voor het verstrekken van persoonsgegevens aan een bestuursorgaan omdat dit voortvloeit uit een wettelijke verplichting, en voor de verwerking van persoonsgegevens door een verantwoordelijke die krachtens de wet belast is met opsporing, omdat dit noodzakelijk is met het oog op de opsporing van strafbare feiten in een bepaald geval.⁴³

Wanneer de gegevensverwerking uitsluitend handmatig plaatsvindt, valt deze verwerking onder het vrijstellingsbesluit. De handmatige gegevensverwerking hoeft dus niet gemeld te worden, tenzij de gegevensverwerking is onderworpen aan een voorafgaand onderzoek.

³⁹ *Kamerstukken II 1997/1998, 25892, nr. 3, p. 86 (MvT).*

⁴⁰ Artikel 17 tot en met 22 Wet bescherming persoonsgegevens.

⁴¹ *Kamerstukken II 1997/1998, 25892, nr. 3, p. 140 (MvT).*

⁴² *Kamerstukken II 1997/1998, 25892, nr. 3, p. 142 (MvT).*

⁴³ 'Handreiking vrijstellingsbesluit', www.cbppweb.nl (zoek op handreiking vrijstellingsbesluit Wbp).

2.4.1. ALGEMENE VEREISTEN

In een aantal gevallen kan de gegevensverwerking niet worden vrijgesteld van de meldplicht. De gegevensverwerking komt niet in aanmerking voor vrijstelling als sprake is van één of meer van de volgende situaties:

- 1) Er is meer dan één verantwoordelijke voor de verwerking;
- 2) Er worden gegevens naar landen buiten de EU doorgegeven;
- 3) De verwerking kent specifieke risico's⁴⁴ en is daarom onderworpen aan een voorafgaand onderzoek;
- 4) De verantwoordelijke heeft ervoor gekozen de gegevensverwerking vrijwillig te melden en heeft dit voornemen ook kenbaar gemaakt. De verantwoordelijke kan ervoor kiezen om de verwerking te melden ondanks dat er sprake is van een vrijstelling van die verwerking. Indien een verantwoordelijke voor een vrijwillige melding heeft gekozen en dit ook te kennen geeft, is er geen weg meer terug. Op dat moment is er geen sprake meer van een vrijstelling en zal de melding aan de wettelijke vereisten moeten voldoen.

2.4.2. CRITERIA VOOR VRIJSTELLING

De Wet bescherming persoonsgegevens geeft een aantal criteria waaraan een gegevensverwerking moet voldoen om onder het vrijstellingsbesluit te vallen. Het College bescherming persoonsgegevens heeft een handreiking opgesteld om te beoordelen of een vrijstelling van toepassing is. Voor vrijstelling moet aan een tweetal voorwaarden zijn voldaan:

- 1) De verwerking voldoet aan de beschrijving van een bepaalde categorie van verwerkingen.
- 2) De verwerking voldoet aan de nadere vereisten voor die bepaalde categorie.

Het Vrijstellingsbesluit noemt verschillende categorieën welke in aanmerking komen voor een vrijstelling. Per categorie wordt in het Vrijstellingsbesluit omschreven voor welke doeleinden gegevensverwerking mag plaatsvinden. Daarnaast geeft het Vrijstellingsbesluit aan welke persoonsgegevens er verwerkt mogen worden en aan wie die gegevens verstrekt mogen worden. Tenslotte wordt per categorie aangegeven hoe lang de betreffende gegevens bewaard mogen worden.

2.5. BURGERLIJK WETBOEK

De grondrechten vinden hun weg naar het arbeidsrecht middels het Burgerlijk Wetboek. De rechter dient op grond van artikel 3:12 van het Burgerlijk Wetboek rekening te houden met algemeen erkende rechtsbeginselen, de in Nederland geldende rechtsovertuigingen en de persoonlijke belangen die in het betreffende geval betrokken zijn. Daartoe behoren ook de grondrechten. Artikel 7:611 van het Burgerlijk Wetboek geeft de arbeidsrechtelijke invulling van de redelijkheid en billijkheid middels het goed werkgever- en werknemerschap.⁴⁵

Werknemers hebben in beginsel recht om in beperkte mate gebruik te maken van de communicatiefaciliteiten op het werk voor persoonlijke doeleinden. Uit een uitspraak⁴⁶ van het EHRM blijkt dat de persoonlijke levenssfeer zich ook uitstrekt tot op de werkplek, maar

⁴⁴ Zie begrippenlijst.

⁴⁵ P.M.H.J. Van Grinsven, H.C. Geugjesen H.N.M. Soemers, 'Arbeidsrecht begrepen', Den Haag: Boom juridische uitgevers, 2009.

⁴⁶ EHRM 25 juni 1997, LJN: AD5858 (Halford/ Verenigd Koninkrijk).

ook tot openbare ruimtes waarmede men redelijkerwijze een bepaalde mate van privacy (*a reasonable expectation of privacy*) mag verwachten. In het onderhavige geval werd de telefoongesprekken van een werknemer afgeluisterd zonder dat dit vooraf aan werknemer kenbaar was gemaakt. Het EHRM oordeelde dat dit in strijd is met artikel 8 van het EVRM. Werknemers moeten ervan uit kunnen gaan dat hun privacy gewaarborgd is. Een 'goed werkgever' dient de persoonlijke levenssfeer van zijn medewerkers te eerbiedigen en mag dus niet zomaar controles uitvoeren. In een uitspraak⁴⁷ van de rechtbank Rotterdam oordeelt de rechter dat wanneer een reglement omtrent het controleren van e-mailberichten ontbreekt het niet wil zeggen dat een werkgever de e-mails niet mag controleren. Er dienen in een dergelijk geval wel extra eisen te worden gesteld aan de controle om te beoordelen of er sprake is van een gerechtvaardigd doel en of is voldaan aan de proportionaliteitstoets. Een werkgever doet er goed aan om een reglement op te stellen zodat hij de proportionaliteit en het doel aan kan tonen. Anderzijds dient een 'goed werknemer' zijn persoonlijke activiteiten op de werkvloer tot in bepaalde mate te beperken, van de werknemer mag in redelijkheid worden verwacht dat hij de grenzen van het toelaatbare kan inzien.⁴⁸

2.6 CONCLUSIE

Niet iedere inbreuk van het recht op eerbiediging van de persoonlijke levenssfeer levert een schending van dat recht op. Er is sprake van een gerechtvaardigde inbreuk op de persoonlijke levenssfeer als die inbreuk voldoet aan de voorwaarden die de Grondwet en het EVRM daaraan stellen. Om te beoordelen of de inbreuk voldoet aan die voorwaarden is wettelijke precisering nodig. De Wet bescherming persoonsgegevens voorziet in regels omtrent de verwerking van persoonsgegevens. In beginsel dient de verwerking van persoonsgegevens gemeld te worden bij het College bescherming persoonsgegevens of de functionaris van de gegevensbescherming. Op deze meldplicht zijn een aantal uitzonderingen. Deze uitzonderingen staan opgesomd in het Vrijstellingsbesluit Wbp. Om een rechtmatige inperking van het recht op privacy van de betrokkene mogelijk te maken dient te worden getoetst aan de Grondwet, het EVRM, de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit.

⁴⁷ Rb. Rotterdam 21 september 2011, nr. 1263172.

⁴⁸ Ktr. Alkmaar 27 juni 2002, nr. 121750/02-1315.

HOOFDSTUK 3

HUIDIGE REGELINGEN

In dit hoofdstuk worden de huidige regelingen op Avans Hogeschool bestudeerd om te beoordelen welke regelingen privacy aspecten in zich bergen. Wanneer de privacy reglementen zijn geïnventariseerd worden deze regelingen vergeleken met huidige wet- en regelgeving omtrent privacy op de werkvloer. Via deze weg wordt een checklist gemaakt van alle privacyaspecten die nog niet voldoende geregeld zijn in het huidige beleid. Tevens wordt uiteengezet hoe Avans in de praktijk omgaat met een aantal privacygevoelige aspecten.

3.1. INTERNET- EN E-MAILGEBRUIK

Gegevens met betrekking tot het e-mail- en internetgebruik van werknemers zijn in het algemeen te kwalificeren als persoonsgegevens. IP-adressen zijn in combinatie met de gebruikersnaam en het wachtwoord te herleiden tot een bepaalde gebruiker. De daaraan verbonden bestanden zijn zodoende herleidbaar tot een werknemer. De verkeersgegevens geven inzicht in de afzender, de bestemming, de datum en de tijd van het bericht of van het internetgebruik.⁴⁹ Met betrekking tot internet- en e-mailverkeer is in vrijwel alle gevallen sprake van verwerking van persoonsgegevens als bedoeld in artikel 1 sub b van de Wet bescherming persoonsgegevens.

Iedere medewerker, wanneer de uitvoering van hun werkzaamheden dit verlangt, heeft toegang tot de ICT- voorzieningen van Avans Hogeschool. In de huisregels worden omtrent het gebruik van de ICT- voorzieningen een aantal regels gesteld. Paragraaf 2.5. van de huisregels⁵⁰ stelt onder andere dat het niet is toegestaan om computervirussen te verspreiden en sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend, opruiend of ander aanstootgevend materiaal tonen. Meer specifiek met betrekking tot het versturen en ontvangen van e-mailberichten is het onder andere niet toegestaan om berichten te zoeken, versturen of laten versturen met racistische, opruiende, aanstootgevende of bedreigende inhoud.

In het kader van privacy is het van belang op welke manier wordt gecontroleerd op het gebruik van de ICT- faciliteiten. De huisregels noemen in paragraaf 2.5. in welke gevallen er gecontroleerd mag worden op het gebruik en hoe deze controles geschieden. De huisregels zijn voor iedere medewerker toegankelijk waardoor zij bekend zijn met het feit dat e-mail en internetgebruik gecontroleerd kan worden. Hiermee is voldaan aan het transparantiebeginsel als bedoeld in artikel 33 en 34 van de Wet bescherming persoonsgegevens.

De directie van de dienst eenheid ICT en facilitaire dienst (hierna: DIF) is gerechtigd om verstuurd en ontvangen berichten en sites te bekijken, te kopiëren of te wissen. Hierbij zijn de gerechtigde personen verplicht tot geheimhouding van inhoud, vorm en strekking van de berichten. Ook systeembeheerders hebben toegang tot deze persoonsgegevens. In artikel 14 van het privacyreglement persoonsgegevens personeel van Stichting Avans⁵¹

⁴⁹ Rb. Rotterdam 29 maart 2001, nr. AW 98/2443-LUG.

⁵⁰ Zie bijlage 1.

⁵¹ Zie bijlage 2.

wordt aan de personen die toegang hebben tot deze persoonsgegevens een geheimhoudingsplicht opgelegd. Op grond van artikel 12 van het privacyreglement dient de systeembeheerder via een coderings- en wachtwoordbeveiliging in het systeem de gerechtigden toegang tot de gewenste persoonsgegevens te verlenen wanneer die toegang is vereist.

Artikel 7 en 8 van de Wet bescherming persoonsgegevens schrijven voor dat persoonsgegevens alleen verwerkt mogen worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Uit de huisregels van Avans blijkt dat het doel is om de naleving van de gebruiksregels te controleren wanneer sprake is van vermoeden van misbruik van de ICT-faciliteiten. Tevens worden controles uitgevoerd om de veiligheid van het netwerk te waarborgen. Bij vermoeden van misbruik of niet naleving van die gebruiksregels mag gecontroleerd worden volgens paragraaf 2.5. van de huisregels van Avans Hogeschool. Tevens worden er van tijd tot tijd controles uitgevoerd.

De algemene bewaartermijn van data is 3 maanden. Na die 3 maanden kunnen de gegevens ook niet meer worden teruggehaald.

De controle op het e-mail en internetverkeer vindt zijn grondslag in artikel 8 sub f van de Wet bescherming persoonsgegevens. Voornoemd artikel stelt dat gegevensverwerking gerechtvaardigd is wanneer de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de werkgever, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

De werkgever dient een aantoonbare belangenafweging te maken tussen zijn belangen en de privacy belangen van zijn werknemers.⁵² De verwerking is alleen toelaatbaar als deze voor de behartiging van het gerechtvaardigd belang noodzakelijk is. Om te beoordelen of de verwerking noodzakelijk is wordt gebruik gemaakt van de zogenoemde 'privacytoets'. Dit zijn vragen die de Memorie van Toelichting⁵³ noemt om een belangenafweging te maken.

1) Is er werkelijk een belang dat de verwerking van persoonsgegevens rechtvaardigt?

In het onderhavige geval is het belang van de werkgever controle op de naleving van de huisregels en de veiligheid van het netwerk waarborgen.

2) Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan, afhankelijk van de ernst van de inbreuk, gegevensverwerking niet achterwege te blijven?

Met de verwerking van de persoonsgegevens wordt inbreuk gemaakt op de persoonlijke levenssfeer van de betrokkene. Wanneer het e-mail- en internetgebruik gecontroleerd wordt, en er dus sprake is van verwerking van persoonsgegevens, kan de directie van DIF controleren op inhoud, vorm en strekking van het gebruik. Tevens zijn zij gerechtigd om de gegevens te kopiëren of te wissen. De ernst van de inbreuk is beperkt doordat er maar een selecte groep over mag gaan tot controle en dus toegang heeft tot de

⁵² J.H.J. Terstegge, 'Goed werken in netwerken - regels voor controle op e-mail en internetgebruik van werknemers', Den Haag, 2002.

⁵³ Kamerstukken II 1997/98, 25 892 (MvT).

gegevens. Tevens rust op de personen die over mogen gaan tot controle een geheimhoudingsplicht waardoor de inbreuk zoveel mogelijk beperkt wordt. De ernst van de inbreuk wordt zodanig ingeperkt dat verwerking daardoor niet achterwege hoeft te blijven.

3) Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg, zonder verwerking, worden bereikt?

Zoals eerder is vermeld is het doel van de verwerking controle op de naleving van de huisregels en de veiligheid van het netwerk waarborgen. In de huisregels wordt vermeld dat inkomend e-mailverkeer op geautomatiseerde wijze gecontroleerd wordt op spam en virussen. Bij deze vorm van controle worden geen persoonsgegevens verwerkt. Op die manier wordt de veiligheid van het netwerk gewaarborgd. Daarentegen zijn er nog vele andere manier die de veiligheid van het netwerk kunnen aantasten. Hiervoor zijn andere maatregelen nodig. Een andere manier om de veiligheid van het netwerk te waarborgen is om het verboden gebruik, welke de huisregels noemen, zoveel mogelijk softwarematig onmogelijk te maken. Zo kunnen bepaalde sites geblokkeerd worden of kan er gebruik gemaakt worden van 'content-filtering'. Dit houdt in dat berichten of bestanden op verboden woorden of extensies worden gescand.⁵⁴ Deze methode kan ook ingezet worden om de naleving van de huisregels te garanderen. Deze methode zal echter niet ieder verboden gebruik kunnen uitsluiten. Zo schrijven de huisregels onder meer voor dat het niet is toegestaan om de computerfaciliteiten te gebruiken voor doeleinden ander dan die welke voortvloeien uit werkzaamheden aan de Hogeschool, dat het medewerkers niet is toegestaan een e-mailadres van iemand anders te gebruiken, anoniem e-mails te versturen of voor andere gebruikers bestemde e-mail te lezen. Om dan toch te kunnen controleren of de huisregels worden nageleefd zullen persoonsgegevens verwerkt dienen te worden. Een deel van het doel dat wordt nagestreefd kan dus zonder verwerking van persoonsgegevens gerealiseerd worden. Helaas kan met voornoemde methode niet ieder verboden gebruik worden uitgesloten en kan de veiligheid van het netwerk niet volledig gewaarborgd worden. Hiervoor is, in bepaalde gevallen, verwerking van persoonsgegevens nodig.

4) Is de verwerking in de mate die is beoogd evenredig aan het nagestreefde doel?

Er wordt alleen overgegaan tot controle van het e-mail- en internetgebruik wanneer sprake is van vermoeden van misbruik van de ICT-faciliteiten. Daarnaast wordt er alleen directe controle uitgevoerd in de werkomgeving van de gebruiker wanneer er gerede aanwijzingen zijn dat er ernstig misbruik wordt gemaakt van de ICT-faciliteiten. Tenslotte zullen er alleen van tijd tot tijd controles worden uitgevoerd om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik in overeenstemming met de huisregels. Als er wordt gecontroleerd is dat alleen wanneer een concrete verdenking van misbruik aanwezig is of er wordt sporadisch gecontroleerd. De controles zijn daarom niet een te zwaar middel om het doel te verwezenlijken. Zij worden zorgvuldig en in voorafgaand bepaalde gevallen uitgevoerd. De verwerking is dan ook evenredig aan het nagestreefde doel. De controle van het e-mail en internetgebruik van medewerkers heeft de privacytoets doorstaan en is daarmee rechtvaardig op grond van artikel 8 sub f van de Wet bescherming persoonsgegevens.

⁵⁴ J.H.J. Terstegge, 'Goed werken in netwerken - regels voor controle op e-mail en internetgebruik van werknemers', Den Haag, 2002.

Zoals in hoofdstuk 2 is vermeld rust er een meldingsplicht op de verantwoordelijke indien er persoonsgegevens worden verwerkt. Bepaalde verwerkingen van persoonsgegevens zijn vrijgesteld van de meldingsplicht. Het Vrijstellingsbesluit bevat een aantal vrijstellingen met betrekking tot het gebruik van computers.

Om te beoordelen of voornoemde verwerkingen van persoonsgegevens in aanmerking komen voor vrijstelling dient getoetst te worden aan de criteria die de artikelen 32 en 34 van het Vrijstellingsbesluit stellen.

Artikel 32 van het Vrijstellingsbesluit is gericht op de verwerking van persoonsgegevens die betrekking heeft op het aanbieden van faciliteiten of diensten op een netwerk aan personen in dienst van of werkzaam voor de verantwoordelijke. Het aanbieden van ICT-faciliteiten aan de werknemers valt dus onder artikel 32 van het Vrijstellingsbesluit. De huisregels noemen als doel voor de verwerking het controleren van de naleving van de huisregels en de veiligheid van het netwerk waarborgen. Hiermee voldoet het doel aan het criteria van toegestane doeleinden als bedoeld in artikel 32 lid 3 onder c van het Vrijstellingsbesluit. Uit de Memorie van Toelichting⁵⁵ blijkt dat voor de verwerking met betrekking tot de interne controle instemming van de ondernemingsraad is vereist. Indien er geen instemming is komt de verwerking niet in aanmerking voor vrijstelling. Uit interviews⁵⁶ blijkt dat de ondernemingsraad heeft ingestemd met de regeling.

Tevens wordt voldaan aan de criteria die artikel 32 lid 4 onder a, b, c en d van het Vrijstellingsbesluit noemt. Er worden alleen persoonsgegevens verwerkt die betrekking hebben op de verrichtingen van de gebruikers en de netwerkbeheerder, er worden gegevens met betrekking tot elektronische berichten afkomstig van of bestemd voor gebruikers verwerkt, en medewerkers hebben een eigen 'username' waarmee ze het netwerk kunnen betreden. Er wordt alleen gecontroleerd op eventueel verboden bezochte sites of verzonden of ontvangen berichten die in strijd zijn met de huisregels. Tevens heeft iedere medewerker een inlogcode waardoor alleen die medewerker het voor hem bestemde netwerk kan betreden.

Doordat alleen de directie van DIF gerechtigd is om de controle uit te voeren is voldaan aan het derde criteria genoemd in artikel 32 lid 5 sub a Vrijstellingsbesluit. De directie van DIF is verantwoordelijk voor de elektronische communicatiedienst als bedoeld in artikel 1.1 sub g van de Telecommunicatiewet. Hierbij is het voornaam dat de persoonsgegevens alleen aan derden worden verstrekt indien de gegevens nodig zijn voor het behandelen van geschillen. In de huisregels staat vermeld dat alleen de directie van DIF toegang heeft tot de persoonsgegevens en dat zij verplicht zijn tot geheimhouding. Er staat niet vermeld in welke gevallen de persoonsgegevens verstrekt mogen worden. Dit staat wel vermeld in artikel 10 van het privacyreglement persoonsgegevens personeel. Daarmee is voldaan aan het vereiste van artikel 32 lid 5 van het Vrijstellingsbesluit.

Het laatste vereiste van artikel 32 lid 6 van het Vrijstellingsbesluit stelt dat persoonsgegevens niet langer dan 6 maanden nadat zij verkregen zijn bewaard mogen worden. Avans Hogeschool hanteert een algemene bewaartermijn van 3 maanden voor data. En valt daarmee binnen de bewaartermijn die het Vrijstellingsbesluit noemt.

⁵⁵ Kamerstukken II 2001/02, 5095178/01/6 (MvT).

⁵⁶ Zij bijlage 3.

3.2. SOCIAL MEDIA

In het kader van internet search worden vrijwel altijd persoonsgegevens verwerkt, de gegevens zijn immers herleidbaar tot een identificeerbare persoon.⁵⁷ Dit is zeker het geval met social media omdat vrijwel iedere pagina een persoon identificeert.

Op het moment is er nog geen social media protocol op Avans Hogeschool. Afgelopen jaar heeft Avans Hogeschool een richtlijn 'spelregels social media' uitgebracht waar zij veel kritiek op heeft ontvangen. Er is een verslag uitgebracht waarin uiteen is gezet waar die kritiek voornamelijk op gegeven werd. Avans Hogeschool heeft als reactie hierop de spelregels teruggetrokken en is momenteel druk bezig om een nieuwe richtlijn te schrijven.

Van alle commotie rondom de vorige richtlijn omtrent social media heeft Avans geleerd. Momenteel is er een concept regeling opgesteld die voornamelijk gericht is op een positieve benadering en die geen verboden oplegt. Avans is erg voorzichtig met het publiceren van een nieuwe richtlijn vandaar dat de conceptregeling niet is opgenomen in dit onderzoeksrapport.

Met de regeling omtrent social media wil Avans helderheid scheppen over wat de mogelijkheden van social media zijn en daarentegen ook wat de consequenties kunnen zijn van bepaald gebruik.

In de regeling is (nog) niets geregeld over hoe de controle van social media gebruik van medewerkers wordt uitgevoerd. Uit het voorgaande interview⁵⁸ blijkt dat deze regeling in de huisregels van Avans zal worden geplaatst onder paragraaf 2.5. deze paragraaf gaat over het gebruik van ICT-voorzieningen zoals ook eerder in dit hoofdstuk is vermeld. De controle zal dan op dezelfde manier geschieden als de controle op de ICT-voorzieningen namelijk door de directie van de dienst eenheid ICT en facilitaire dienst. Er mag volgens die huisregels sporadisch of bij vermoeden van misbruik gecontroleerd worden. Ook de beveiliging en bewaartermijn van de gegevens en de personen over wie persoonsgegevens verwerkt mogen worden zijn dezelfde als bij het ICT-gebruik.

De controle op social media gebruik vindt zijn grondslag in artikel 8 sub f van de Wet bescherming persoonsgegevens. Voornoemd artikel stelt dat gegevensverwerking gerechtvaardigd is wanneer de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de werkgever, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

De werkgever dient een aantoonbare belangenafweging te maken tussen zijn belangen en de privacy belangen van zijn werknemers.⁵⁹ De verwerking is alleen toelaatbaar als deze voor de behartiging van het gerechtvaardigde belang noodzakelijk is. De Memorie van Toelichting biedt een aantal vragen om te bepalen welk belang prevaleert.

⁵⁷ 'Q&A over privacy, social media en de werkplek', ArbeidsRecht 2012/34.

⁵⁸ Zie bijlage 3.

⁵⁹ J.H.J. Terstegge, 'Goed werken in netwerken - regels voor controle op e-mail en internetgebruik van werknemers', Den Haag, 2002.

1) Is er werkelijk een belang dat de verwerking van persoonsgegevens rechtvaardigt?

In het geval van controle op social media is het belang van de werkgever controle op de naleving van de huisregels en de veiligheid van het netwerk waarborgen.

2) Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan, afhankelijk van de ernst van de inbreuk, gegevensverwerking niet achterwege te blijven?

Met de verwerking van de persoonsgegevens wordt inbreuk gemaakt op de persoonlijke levenssfeer van de betrokkene. Wanneer het social media gebruik van werknemers wordt gecontroleerd worden er persoonsgegevens van de betreffende werknemer verwerkt. Dit maakt een inbreuk op de persoonlijke levenssfeer van de betrokkene. De ernst van de inbreuk kan beperkt worden door alleen berichten te controleren die op de openbare delen van social media worden geplaatst. Deze berichten zijn immers voor iedereen toegankelijk en de betrokkene is zich daar ook van bewust. Gegevensverwerking hoeft daarom niet achterwege te blijven.

3) Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg, zonder verwerking, worden bereikt?

Zoals eerder is vermeld is het doel van de verwerking controle op de naleving van de huisregels en de veiligheid van het netwerk waarborgen. Social media sites zijn sites die een individu zelf beheert en waar anderen toegang tot hebben. Om te controleren of er geen social media gebruik plaatsvindt dat in strijd is met de huisregels zal de pagina van een bepaalde werknemer gecontroleerd dienen te worden. Dit kan niet op een manier zonder verwerking van persoonsgegevens geschieden, om te controleren heeft men zich namelijk al toegang tot de pagina van de betrokkene verschaft.

4) Is de verwerking in de mate die is beoogd evenredig aan het nagestreefde doel? De controle op social media geschiedt op dezelfde wijze als de controle op e-mail- en internetgebruik. Als er wordt gecontroleerd is dat dus alleen wanneer een concrete verdenking van misbruik aanwezig is of er wordt sporadisch gecontroleerd. De controles zijn daarom niet een te zwaar middel om het doel te verwezenlijken. Zij worden zorgvuldig en in voorafgaand bepaalde gevallen uitgevoerd. De verwerking is dan ook evenredig aan het na te streven doel.

De controle van het social mediagebruik van medewerkers heeft de privacytoets doorstaan en is daarmee rechtvaardig op grond van artikel 8 sub f van de Wet bescherming persoonsgegevens.

De huisregels noemen als doel voor de verwerking van voornoemde persoonsgegevens het controleren van de naleving van de huisregels en de veiligheid van het netwerk waarborgen. Hiermee voldoet het doel aan het criteria van toegestane doeleinden als bedoeld in artikel 32 lid 3 onder c van het Vrijstellingsbesluit. Uit de Memorie van Toelichting⁶⁰ blijkt dat voor de verwerking met betrekking tot de interne controle instemming van de ondernemingsraad is vereist. Wanneer wordt overgegaan tot het invoeren van een gedragscode voor social media en er is een regeling omtrent het monitoren van social media van werknemers dan is daarvoor dus instemming van de ondernemingsraad

⁶⁰ Kamerstukken II 2001/02, 5095178/01/6 (MvT).

vereist.⁶¹

Doordat alleen de directie van DIF gerechtigd is om de controle uit te voeren is voldaan aan het derde criteria genoemd in artikel 32 lid 5 sub a Vrijstellingsbesluit. De directie van DIF is verantwoordelijk voor de elektronische communicatiedienst als bedoeld in artikel 1.1 sub g van de Telecommunicatiewet. Hierbij is het voornaam dat de persoonsgegevens alleen aan derden worden verstrekt indien de gegevens nodig zijn voor het behandelen van geschillen. In de huisregels staat vermeld dat alleen de directie van DIF toegang heeft tot de persoonsgegevens en dat zij verplicht zijn tot geheimhouding. Er staat niet vermeld in welke gevallen de persoonsgegevens verstrekt mogen worden. Dit staat wel vermeld in artikel 10 van het privacyreglement persoonsgegevens personeel. Daarmee is voldaan aan het vereiste van artikel 32 lid 5 van het Vrijstellingsbesluit.

Het laatste vereiste van artikel 32 lid 6 van het Vrijstellingsbesluit stelt dat persoonsgegevens niet langer dan 6 maanden nadat zij verkregen zijn bewaard mogen worden.

3.3. CAMERATOEZICHT

Studenten en medewerkers worden bij binnenkomst geobserveerd door verschillende camera's. De camerabeelden kunnen gegevens bevatten die herleiden naar een identificeerbare persoon, er is dus sprake van een persoonsgegeven in de zin van de Wet bescherming persoonsgegevens. Er wordt gebruik gemaakt van digitale videotechneek. Dat wil zeggen dat beeld en geluid opgeslagen worden op bijvoorbeeld een harde schijf.⁶² Digitaal cameratoezicht valt onder de reikwijdte van de Wet bescherming persoonsgegevens.

Een ieder die een gebouw van Avans betreedt wordt geobserveerd door videocamera's. Op de servicebalies en receptiebalies worden uitsluitend real-time beelden bekeken. Wanneer er een incident wordt waargenomen of is voorgevallen, is binnen Avans Hogeschool de directeur van de dienst eenheid ICT en facilitaire dienst vanuit het College van Bestuur gemandateerd om de camerabeelden terug te kijken. Het cameratoezicht wordt op elke locatie kenbaar gemaakt middels een bord bij de ingang waarop staat vermeld dat er video observatie plaatsvindt. (zie figuur 1).

Figuur 1 Cameratoezicht vindt net als de controle op e-mail- en internetgebruik zijn grondslag in artikel 8 sub f van de Wet bescherming persoonsgegevens. Dit betekent dat het cameratoezicht noodzakelijk moet zijn voor de behartiging van het gerechtvaardigde belang van de werkgever. Hierbij dient tevens een belangenafweging plaats te vinden tussen het belang van de werkgever en het belang van de bescherming van de persoonlijke levenssfeer van de werknemer.

⁶¹ E. Thole en A. Engelfriet, 'Q&A over privacy, social media en de werkplek', ArbeidsRecht, 34, nr. 8/9, 2012.

⁶² CBP, 'Regels voor cameratoezicht', www.cbppweb.nl (zoek op: regels voor cameratoezicht).

Figuur 1:



Om te voldoen aan de regels van de Wet bescherming persoonsgegevens moet vooraleerst het doel van het cameratoezicht zijn vastgelegd. Momenteel is er nog geen specifiek beleid omtrent cameratoezicht maar er is een concept privacyreglement persoonsgegevens personeel Stichting Avans⁶³ opgesteld. Deze conceptregeling wordt zeer binnenkort ingevoerd. In dit privacyreglement zijn een aantal algemene bepalingen opgenomen omtrent de verwerking van persoonsgegevens. Uit artikel 7 sub o van die regeling blijkt dat deze regeling ook geldt voor cameratoezicht. Zo worden in artikel 4 van het reglement doelstellingen genoemd voor de verwerking van persoonsgegevens. De regeling noemt de volgende doelen die betrekking hebben op het cameratoezicht: het behandelen van geschillen en het creëren van een veilige omgeving voor medewerkers en studenten. Het cameratoezicht is voornamelijk preventief. Er is dus een belang dat het cameratoezicht rechtvaardigt. Het Vrijstellingsbesluit heeft omtrent cameratoezicht eveneens een aantal criteria opgesomd. Uit artikel 38 lid 2 van het Vrijstellingsbesluit blijkt dat de bescherming van de veiligheid van natuurlijke personen en het vastleggen van incidenten verwerkingen zijn die onder de reikwijdte van het Vrijstellingsbesluit vallen.

Met het cameratoezicht wordt inbreuk gemaakt op de persoonlijke levenssfeer van betrokkenen maar de inbreuk wordt zoveel mogelijk beperkt. Zo zijn de beelden bij de recepties en servicebalies alleen maar real-time beschikbaar. Wanneer sprake is van een incident zoals diefstal is uitsluitend de directeur van de dienst eenheid ICT en facilitaire dienst bevoegd om de camerabeelden terug te kijken. Indien er gegevens aan derden worden verstrekt is dat, op grond van artikel 10 lid 2 en lid 3 van het privacyreglement persoonsgegevens personeel, met het oog op de bedrijfsbeveiliging, behandelen van geschillen of de gegevens worden aan opsporingsambtenaren verstrekt indien de gegevens daartoe aanleiding geven. Hiermee wordt tevens voldaan aan het criterium dat artikel 38 lid 5 van het Vrijstellingsbesluit noemt. Daarnaast is de ernst van de inbreuk

⁶³ Zie bijlage 2.

zodanig ingeperkt dat cameratoezicht niet achterwege hoeft te blijven. Het doel van het cameratoezicht kan niet op een andere manier, zonder cameratoezicht, bereikt worden. Om geschillen te behandelen zoals een verzekeringskwestie bij diefstal zijn camerabeelden nodig voor de bewijslast. Doordat de camera's voornamelijk als preventieve maatregel aanwezig zijn wordt een veilige omgeving gecreëerd voor medewerkers en studenten. Wanneer er het bewustzijn is dat men gefilmd wordt zal in het algemeen minder criminaliteit plaatsvinden.

Camerabeelden worden binnen Avans Hogeschool op grond van artikel 15 lid 7 van het privacyreglement persoonsgegevens personeel niet langer bewaard worden dan noodzakelijk is voor het doel waarvoor ze verzameld. De gegevens worden na een termijn van 14 dagen vernietigd, dan wel na afhandeling van de geconstateerde incidenten. Met deze termijn is voldaan aan het criterium van vier weken dat artikel 38 lid 6 van het Vrijstellingsbesluit stelt. Tenslotte heeft de ondernemingsraad bij de realisatie van de gebouwen ingestemd met cameratoezicht.

3.4. TELEFOONGEBRUIK

Medewerkers van Avans Hogeschool maken gebruik van ofwel een mobiele telefoon ofwel van een vaste telefoon. In beginsel is het telefoongebruik van medewerkers zakelijk gebruik. Maar dat wil niet zeggen dat een privé telefoongesprek niet is toegestaan. Avans controleert niet welke gesprekken zakelijk of privé zijn. Hieromtrent is dan ook geen schriftelijke regeling opgesteld.

Avans Hogeschool ontvangt van KPN een rapportage waar ook individuele gegevens in opgenomen zijn. De informatie over telefoongesprekken die door de telefooncentrale wordt verstrekt worden vallen onder de reikwijdte van de Wet bescherming persoonsgegevens, er is namelijk sprake van geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen. De gegevens worden door Avans niet met een specifiek doel verwerkt, werknemers kunnen hun eigen gegevens inzien om bijvoorbeeld een nummer op te zoeken. KPN verzamelt de gegevens en verstrekt ze vervolgens aan Avans.

De verwerking van telefoongegevens vindt zijn grondslag in artikel 8 sub b van de Wet bescherming persoonsgegevens. Voornoemd artikel stelt dat het verwerken van persoonsgegevens gerechtvaardigd is als de gegevensverwerking noodzakelijk is voor de uitvoering van de overeenkomst waarbij de betrokkene partij is. Avans Hogeschool heeft een overeenkomst met de telefooncentrale (KPN). Om de kosten in kaart te brengen worden de telefoongegevens verwerkt. Binnen Avans is er één persoon die de gegevens in kan zien. Tevens kunnen medewerkers bij deze persoon een verzoek doen om hun eigen gegevens in te zien. Alleen een verzoek van inzien van eigen gegevens wordt gehonoreerd. Indien een leidinggevende de gegevens van één van zijn medewerkers wil inzien dan wordt het verzoek niet gehonoreerd. De gegevens van mobiele telefonie worden 24 maanden in een database bewaard. Bij vaste telefonie worden de gegevens maar 1 maand bewaard.

Om te beoordelen of er van het verwerken van de telefoongegevens melding moet worden gedaan, wordt getoetst aan artikel 34 van het Vrijstellingsbesluit. De verwerking geschiedt alleen voor het verzenden van mondelinge of schriftelijke boodschappen, de telefoongegevens moeten verwerkt worden om een telefoonconnectie te krijgen om een gesprek te kunnen voeren. Tevens zijn de gegevens nodig om een verbinding tussen beiden telefoontoestellen te kunnen maken. Hiermee is voldaan aan het criterium dat artikel 34 lid

2 sub a en sub b van het Vrijstellingsbesluit stelt.

Daarnaast worden alleen telefoongegevens verwerkt waarop alleen datum, begin- en eindtijd van het gesprek en telefoonnummer staan vermeld. Dit is in overeenstemming met artikel 34 lid 3 sub a en b van het Vrijstellingsbesluit.

Tenslotte worden de mobiele telefoongegevens 24 maanden bewaard en de vaste telefoniegegevens 1 maand. Artikel 34 lid 5 van het Vrijstellingsbesluit stelt dat voornoemde persoonsgegevens niet langer dan 6 maanden bewaard mogen worden. De bewaartermijn van 1 maand voor vaste telefoniegegevens is dus in overeenstemming met de wetgeving maar de bewaartermijn van 24 maanden overschrijdt de door het Vrijstellingsbesluit voorgeschreven bewaartermijn. Tevens dient er een schriftelijke regeling te worden opgesteld met betrekking tot hoe lang de gegevens bewaard blijven en wie bevoegd is tot inzage van de gegevens om in overeenstemming met het transparantiebeginsel te handelen als bedoeld in artikel 33 en 34 van de Wet bescherming persoonsgegevens.

3.5. NIEUWE HRM-SYSTEEM

Binnenkort wordt er een nieuwe HRM procedure gestart. Deze nieuwe procedure betreft een nieuwe methode omtrent de personeelsadministratie. De bij deze procedure betrokken persoonsgegevens zijn onder andere naam, adres, salaris, belastinggroep, burgerlijke staat, foto, curriculum vitae, et cetera. De persoonsgegevens zijn in een bestand opgenomen en met de nieuwe procedure zal het grootste deel van de personeelsadministratie geautomatiseerd geschieden. Op grond van artikel 2 lid 1 van de Wet bescherming persoonsgegevens is de Wet bescherming persoonsgegevens dus van toepassing op de personeelsadministratie. Een beleid rondom de nieuwe procedure is nog niet ontwikkeld.

De nieuwe procedure houdt vooral in dat het huidige systeem uitgebreid wordt met self service procedures. Het gaat over procedures als werving en selectie tot en met ontslag, arbeidsvoorwaarden en meer. Het is de bedoeling dat medewerkers eigen persoonsgegevens kunnen invoeren in het systeem zodat dat niet meer centraal door de afdeling DP&O hoeft te worden gedaan. Een medewerker kan met het nieuwe systeem bijvoorbeeld zelf een adreswijziging invoeren of managers kunnen zelf online de gegevens van een nieuwe medewerker invoeren. De controle van de gegevens wordt daarbij, zoals voorheen ook het geval was, door de afdeling DP&O uitgevoerd.

Op het moment maakt Avans gebruik van papieren personeelsdossiers. Met de nieuwe procedure wordt het personeelsdossier digitaal en is het mogelijk dat een medewerker zijn eigen personeelsdossier online kan raadplegen. De afdeling is momenteel druk bezig om ervoor te zorgen dat de online personeelsdossiers alleen door de bevoegde persoon geraadpleegd kunnen worden. Het HRM-systeem wordt pas ingevoerd als men ervan overtuigd is dat de privacy, in relatie tot het systeem en de autorisaties die daarmee gemoeid zijn, goed gewaarborgd is.

Een manager kan met de nieuwe procedure de basale zaken inzien van de medewerkers die onder hem vallen. Een manager heeft met de nieuwe procedure online toegang tot gegevens zoals onder andere leeftijd, salaris en rapportages van functioneringsgesprekken. Deze gegevens kan een manager momenteel ook inzien maar die gegevens worden door de afdeling DP&O geleverd. Tevens is er een groep administrateurs die toegang hebben tot de gegevens. Medische gegevens worden niet verstrekt.

De bewaartermijn, van de persoonsgegevens die verwerkt worden met het nieuwe systeem, is nog niet vastgesteld. Doordat er verschillende soorten gegevens verwerkt worden dient rekening te worden gehouden met verschillende bewaartermijn per categorie persoonsgegevens. Avans is nog in discussie over wat de daadwerkelijke bewaartermijnen zullen worden, het streven is om in ieder geval aan de wettelijke bepalingen te voldoen.

Buiten de werknemer zelf, en in voorafgaand bepaalde gevallen de leidinggevende, heeft ook een groep administrateurs toegang tot de persoonsgegevens van de werknemers. Om de privacy te waarborgen is hun op grond van het privacy reglement persoonsgegevens personeel een geheimhoudingsplicht opgelegd.

Het verwerken van persoonsgegevens in het kader van personeelsadministratie vindt zijn grondslag in artikel 8 sub b van de Wet bescherming persoonsgegevens. De gegevens die verwerkt worden zijn noodzakelijk voor de uitvoering van de arbeidsovereenkomst. Zonder onder andere een naam, adres en bankrekeningnummer kan er geen arbeidsovereenkomst tot stand komen. Op grond van artikel 11 van de Wet bescherming persoonsgegevens is het van belang dat de hoeveelheid persoonsgegevens beperkt wordt tot de absoluut noodzakelijke gegevens die nodig zijn voor de uitvoering van de arbeidsovereenkomst.

Artikel 7 van het Vrijstellingsbesluit stelt tevens een aantal criteria met betrekking tot de personeelsadministratie om voor vrijstelling van de meldplicht in aanmerking te komen. In lid 2 van voornoemd artikel worden verscheidene doeleinden genoemd. Uit het privacyreglement persoonsgegevens personeel⁶⁴ blijkt dat de persoonsgegevens voor de volgende doeleinden worden verwerkt:

- de behandeling van personeelszaken door de Dienst eenheid Personeel & Organisatie;
- het geven van leiding aan de werkzaamheden van de betrokkene;
- het berekenen vaststellen, vastleggen en doen uitbetalen van salarisaanspraken, vergoedingen en andere geldsommen en beloningen in natura aan of ten behoeve van betrokkenen;
- het berekenen vastleggen en betalen van belasting en premies ten behoeve van de betrokkene;
- het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband;
- de opleiding van de betrokkene;
- de bedrijf medische zorg voor de betrokkene;
- het bedrijfsmaatschappelijk werk;
- de verkiezing van de leden van een bij wet geregeld medezeggenschapsorgaan;
- de interne controle en de bedrijfsbeveiliging;
- de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarden;
- het verlenen van ontslag;
- de administratie van de personeelsvereniging en van de vereniging van oud-personeelsleden;
- het innen van vorderingen, met inbegrip van het in handen van derden stellen van de vorderingen;
- het behandelen van geschillen;
- het doen uitoefenen van de accountantscontrole;

⁶⁴Zie bijlage 2.

- de overgang van de betrokkene naar of de tijdelijke tewerkstelling van de betrokkene bij een ander onderdeel van de groep waaraan het College van Bestuur is verbonden;
- de uitvoering of toepassing van een andere wet;
- het creëren van een veilige omgeving voor medewerkers en studenten;
- het (laten) uitvoeren van onderzoeken op het gebied van medewerkerstevredenheid, werkdruk onder werknemers of soortgelijke onderwerpen die voor de organisatie van belang zijn.

De hiervoor beschreven doeleinden komen overeen met de beschreven doeleinden in artikel 7 lid 2 respectievelijk sub b, a, c, d, e, f, g, h, i, j, l, m, n, o, p, q van het Vrijstellingsbesluit.

Het doeleinde dat niet in het Vrijstellingsbesluit staat beschreven is het (laten) uitvoeren van onderzoeken op het gebied van medewerkerstevredenheid, werkdruk onder werknemers of soortgelijke onderwerpen die voor de organisatie van belang zijn.

Artikel 7 van het privacyreglement personeelsgegevens van Avans benoemt welke soort gegevens verwerkt worden. Het artikel stemt overeen met artikel 7 lid 3 van het Vrijstellingsbesluit. Er worden dus geen andere persoonsgegevens verwerkt dan diegene die in het Vrijstellingsbesluit genoemd zijn om in aanmerking te komen voor vrijstelling van de meldplicht.

In artikel 12 van het privacyreglement persoonsgegevens Avans wordt benoemd welke personen toegang hebben tot de persoonsgegevens van het personeel. Dit zijn:

- het College van Bestuur of diens mandant;
- de beheerder;
- de door de beheerder aangewezen bewerker voor de persoonsgegevens over de tot zijn/haar werkgebied behorende betrokkenen;
- de systeembeheerders.

Bovengenoemde personen zijn belast met of geven leiding aan de activiteiten die in artikel 4 van het privacyreglement zijn beschreven en die eerder in dit hoofdstuk al omschreven zijn. De systeembeheerders zijn noodzakelijk betrokken bij de activiteiten vanwege hun functie. Zij hebben vanwege hun functie automatisch toegang tot de informatie die de systemen bevatten omdat zij verantwoordelijk zijn voor de goede werking van computer- en/of andere systemen. Deregeling voldoet aan de norm van artikel 7 lid 4 onder a van het Vrijstellingsbesluit.

Tot slot stelt het Vrijstellingsbesluit dat de persoonsgegevens maximaal twee jaren mogen worden bewaard tenzij moet worden voldaan aan een andere wettelijke bewaarplicht. Ook de algemeen gehanteerde bewaarplicht van twee jaar die Avans hanteert is in overeenstemming met voornoemd artikel zo blijkt uit artikel 15 van het privacyreglement personeelsgegevens Avans.

3.6. CONCLUSIE

Uit het voorgaande kan geconcludeerd worden dat de controle op het e-mail en internetgebruik de persoonlijke levenssfeer van medewerkers voldoende waarborgd. De regeling voldoet aan de vereisten die de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit stellen. Doordat ook aan de vereisten van het Vrijstellingsbesluit is voldaan is de verwerking van voornoemde persoonsgegevens vrijgesteld van de meldplicht als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens. Wanneer de social media richtlijn ingevoerd wordt zal deze aan dezelfde regels gebonden zijn die gelden voor het ICT-gebruik. Dat wil zeggen dat de controle daarop net als de controle op

het e-mail en internetgebruik voldoet aan de vereisten van de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit. Omdat de regeling nog niet volledig is dient na de invoering van de definitieve regeling getoetst te worden of alle aspecten van die regeling ook voldoen aan het wettelijk kader zoals hiervoor omschreven is.

Het cameratoezicht op Avans Hogeschool voldoet aan de noodzakelijkheidstoets van artikel 8 sub f van de Wet bescherming persoonsgegevens. Dat wil zeggen dat het belang van de werkgever in dit geval prevaleert boven het belang van de werknemer. De inbreuk op de persoonlijke levenssfeer is niet van zodanige aard dat er van cameratoezicht afgezien hoeft te worden. Tevens voldoet het cameratoezicht aan de vereisten van het Vrijstellingsbesluit omtrent cameratoezicht. Dus kan er worden geconstateerd dat Avans Hogeschool vrijgesteld is van de meldplicht als het gaat om cameratoezicht.

De verwerking van telefoongegevens voldoet aan de vereisten van artikel 8 sub b van de Wet bescherming persoonsgegevens. De verwerking van vaste telefoniegegevens voldoet tevens aan de vereisten van het Vrijstellingsbesluit. De mobiele telefoniegegevens worden 24 maanden bewaard. Deze bewaartermijn overschrijdt de bewaartermijn die het Vrijstellingsbesluit voorschrijft. Tevens is de bewaartermijn niet noodzakelijk ter voldoening aan een wettelijke bewaarplicht. Dat wil zeggen dat de bewaartermijn van de mobiele telefoniegegevens te lang is en daardoor is Avans niet vrijgesteld van de meldplicht omtrent de verwerking van mobiele telefoniegegevens.

Tenslotte wordt binnenkort een nieuwe HRM procedure gestart die ervoor moet zorgen dat de personeelsadministratie voor een gedeelte door werknemers zelf of door leidinggevenden kan worden ingevoerd. Het privacyreglement persoonsgegevens personeel voldoet aan de vereisten die door de Wet bescherming persoonsgegevens worden gesteld aan de personeelsadministratie. Tevens voldoet de regeling aan het Vrijstellingsbesluit. Hieruit kan geconcludeerd worden dat de nieuwe HRM procedure is vrijgesteld van de meldplicht als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens.

HOOFDSTUK 4

WAT MOET AVANS DOEN OM DE PRIVACY VAN WERKNEMERS TE WAARBORGEN?

Aan de hand van de voorgaande hoofdstukken wordt bepaald wat Avans nog moet doen om de persoonlijke levenssfeer van het personeel voldoende te waarborgen.

4.1. SOCIAL MEDIA

Momenteel is er nog geen social media richtlijn ingevoerd. De regeling dient zodanig te worden opgesteld dat de persoonlijke levenssfeer van de werknemers voldoende gewaarborgd is. De werkgever kan voorschriften stellen ter bevordering van de goede orde binnen het bedrijf en de uitvoering van het werk.⁶⁵ Uit jurisprudentie blijkt dat wanneer een werknemer grove beledigingen of racistische berichten over bijvoorbeeld zijn leidinggevende of collega op social media plaatst, dit reden kan zijn tot ontslag. Daarbij is het wel van belang dat wanneer de werknemer die zulke berichten heeft geplaatst een officiële waarschuwing krijgt alvorens tot ontslag wordt overgegaan.⁶⁶

In de concept social media richtlijn worden een aantal richtlijnen opgesomd voor een juist gebruik van social media. Daarnaast worden zogenaamde 'dont's' genoemd. Het is van belang dat de social media richtlijn geen totaalverbod, op uitingen die betrekking hebben op het werk, oplegt dit zou in strijd zijn met de vrijheid van meningsuiting.

In de richtlijn wordt niet vermeld in hoeverre werknemers social media voor privédoeleinden onder werktijd mogen gebruiken. Dit is geen vereiste maar in de social media code mag worden bepaald dat werknemers social media voor privé doeleinden mogen gebruiken zolang het werk daar niet onder lijdt. Het in bepaalde mate inperken van social media gebruik is dus mogelijk.

De controle op social media gebruik zal op dezelfde wijze geschieden als de controle van het ICT-gebruik zoals in de huisregels staat vermeld. Dat wil zeggen dat de directie van DIF bevoegd is om sporadisch te controleren en dat er gecontroleerd wordt met hetzelfde doel: controle op de naleving van de huisregels en de veiligheid van het netwerk waarborgen. De directie van DIF heeft volgens de huisregels toegang tot de inhoud, vorm en strekking van berichten. Om de inbreuk op de persoonlijke levenssfeer van de werknemer zoveel mogelijk te beperken is het raadzaam om in de regeling op te nemen dat alleen berichten die op openbare delen van sociale media worden geplaatst zullen worden gecontroleerd. Daarbij is het nog steeds zeer van belang dat dit sporadisch gebeurt en dat alle regels die de Wet bescherming persoonsgegevens aan de verwerking van persoonsgegevens stelt in acht worden genomen. Daarnaast mogen de gegevens die met de controle verkregen zijn maximaal 6 maanden nadat zij zijn verkregen bewaard worden om in aanmerking te komen voor vrijstelling van de meldplicht.

Wanneer wordt overgegaan tot het invoeren van een gedragscode voor social media en er is een regeling omtrent het monitoren van social media van werknemers dan is daarvoor

⁶⁵ E. Thole en A. Engelfriet, 'Q&A over privacy, social media en de werkplek', ArbeidsRecht, 34, nr. 8/9, 2012.

⁶⁶ Rb. Arnhem, sector kanton, 19 maart 2012, LJN BV9483 (Blokker).

Rb. Arnhem, sector kanton Wageningen, 11 april 2012, L/N BW2006 (JK Vloerverwarming).

instemming van de ondernemingsraad vereist.⁶⁷

4.2. TELEFOONGEBRUIK

In hoofdstuk 3 is vermeld dat de bewaartermijn van mobiele telefoniegegevens bij Avans 24 maanden is. Deze bewaartermijn voldoet niet aan de bepalingen van het Vrijstellingsbesluit. Om hieraan te voldoen dient de bewaartermijn verlaagd te worden naar 6 maanden.

Als Avans de bewaartermijn van de mobiele telefoniegegevens verlaagt naar 6 maanden voldoet zij aan de vereisten van artikel 34 lid 5 van het Vrijstellingsbesluit. Dan zijn zij vrijgesteld van de meldplicht die artikel 27 van de Wet bescherming persoonsgegevens oplegt.

Tevens dient er een schriftelijke regeling te worden opgesteld met betrekking tot hoe lang de gegevens bewaard blijven en wie bevoegd is tot inzage van de gegevens om in overeenstemming met het transparantiebeginsel te handelen als bedoeld in artikel 33 en 34 van de Wet bescherming persoonsgegevens.

4.3. HRM SYSTEEM

Uit hoofdstuk 3 blijkt dat persoonsgegevens in het kader van personeelsadministratie voor verscheidene doeleinden worden verzameld. Uit het interview⁶⁸ omtrent het nieuwe HRM systeem blijkt dat het nog niet duidelijk is welke bewaartermijnen gelden voor de verschillende soorten persoonsgegevens die in de personeelsadministratie zijn opgenomen. Het vrijstellingsbesluit geeft aan dat persoonsgegevens maximaal twee jaren mogen worden bewaard tenzij moet worden voldaan aan een andere wettelijke bewaarplicht.

Om te bepalen welke bewaartermijn geldt voor de persoonsgegevens wordt bekeken voor welke doeleinden de gegevens worden bewaard. Per doelstelling wordt benoemd wat voor persoonsgegevens voor dat doel verwerkt zullen worden en welke bewaartermijn voor die gegevens gehanteerd moet worden.

De algemene wet op de Rijksbelasting is van toepassing op alle werkgevers. Voornoemde wet bepaald hoe lang bepaalde documenten bewaard moeten worden. Voor sommige gegevens uit een personeelsdossier bestaan geen wettelijke bewaartermijnen. Voor die gegevens geldt over het algemeen een bewaartermijn van twee jaar nadat het dienstverband is beëindigd.⁶⁹ In onderstaande tabel wordt een overzicht gegeven van de wettelijke bewaartermijnen die gelden voor verschillende persoonsgegevens.⁷⁰

⁶⁷ E. Thole en A. Engelfriet, 'Q&A over privacy, social media en de werkplek', ArbeidsRecht, 34, nr. 8/9, 2012.

⁶⁸ Zie bijlage 3.

⁶⁹ CBP, 'Bewaartermijnen van persoonsgegevens in uw bestanden', informatieblad nr. 11a, juli 2012, www.cbpweb.nl.

⁷⁰ Tuxx, 'Bewaartermijn personeelsdossier', www.tuxx.nl (zoek op bewaartermijn personeelsdossier).

Doel (privacyreglement persoonsgegevens Avans)	Persoonsgegevens	Bewaartermijn	Wettelijke grondslag
De behandeling van personeelszaken door de Dienst eenheid Personeel & Organisatie	- Sollicitatiegegevens - Arbeidsovereenkomst - Wijziging van arbeidsovereenkomst -Loonbelasting-Verklaringen en kopie identiteitsbewijs -correspondentie inzake benoemingen, promotie, demotie - Afstandsverklaring woon-werkverkeer - Gegevens inzake etniciteit en herkomst - Identiteitspapieren van derden ingeleende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend	- vier weken zonder toestemming van de sollicitant of 1 jaar met toestemming van de sollicitant na de beëindiging van de sollicitatie- procedure - maximaaltweejaarna het einde van het dienstverband - maximaaltweejaarna het einde van het dienstverband - minimaal 5 jaar na het einde van het dienstverband - maximaaltweejaarna het einde van het dienstverband -duur afspraak + 7 jaar - minimaal 5 jaar na het einde van het dienstverband - minimaal 5 jaar na het einde van het dienstverband	- Artikel 5 van het Vrijstellingsbesluit Wbp - artikel 52 Algemene Wet inzake Rijksbelastingen - artikel 52 Algemene Wet inzake Rijksbelastingen -artikel 23a van de uitvoerings-regeling loonbelasting -artikel 52 Algemene Wet inzake Rijksbelastingen - artikel 52 Algemene Wet inzake Rijksbelastingen -Wet stimulering arbeidsdeelname minderheden -Wet arbeid vreemdelingen

het geven van leiding aan de werkzaamheden van de betrokkene	- Verslagen functionerings- en beoordelingsgesprekken - Correspondentie directie / PZ / direct leidinggevende	- maximaaltweejaarna het einde van het dienstverband - einde dienstverband of tot maximaal twee jaar daarna	-vrijstellingsbesluit
het berekenen vastleggen en betalen van belasting en premies ten behoeve van de betrokkene	-loonbeslagen	-tot opheffing	-vrijstellingsbesluit
het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband	-VUT-regeling	-maximaaltweejaarna het einde van het dienstverband	-artikel 52 Algemene Wet inzake Rijksbelastingen
de opleiding van de betrokkene	- Afspraken inzake opleidingen	-periode dat werknemer eventueel nog kosten moet vergoeden	-vrijstellingsbesluit
de bedrijf medische zorg voor de betrokkene	- Ziektekosten - Correspondentie met UWV en de bedrijfsarts	-duurverzekering tot einde van het dienstverband -maximaaltweejaarna het einde van het dienstverband	-vrijstellingsbesluit -vrijstellingsbesluit
de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarden	-Aanvullende arbeids- en salarisafspraken	- minimaal 7 jaar na het einde van het dienstverband	-vrijstellingsbesluit
het verlenen van ontslag	-correspondentie inzake ontslag	-maximaaltweejaarna het einde van het dienstverband	-artikel 52 Algemene Wet inzake Rijksbelastingen
het behandelen van geschillen	- Verslaglegging van probleemsituaties	-maximaaltweejaarna het einde van het dienstverband	-vrijstellingsbesluit
het doen uitoefenen van de accountantscontrole	- Verslaglegging van financiële problemen	-maximaaltweejaarna het einde van het dienstverband	-vrijstellingsbesluit

Als Avans bovenstaande bewaartermijnen hanteert voldoet zij aan het vereiste van het vrijstellingsbesluit en is de verwerking van die persoonsgegevens vrijgesteld van de meldplicht.

Tenslotte noemt het privacyreglement een doelstelling die niet in het Vrijstellingsbesluit genoemd wordt: het (laten) uitvoeren van onderzoeken op het gebied van medewerkerstevredenheid, werkdruk onder werknemers of soortgelijke onderwerpen die voor de organisatie van belang zijn. Om toch te kunnen voldoen aan de vereisten van het Vrijstellingsbesluit en de vereisten van de Wet bescherming persoonsgegevens kan Avans

ervoor zorgen dat voornoemde onderzoeken anoniem worden afgenomen. Op die manier worden er geen persoonsgegevens verwerkt en is de privacy van de werknemers gewaarborgd.

4.4. FUNCTIONARIS VOOR DE GEGEVENS BESCHERMING

Binnen Avans Hogeschool is een privacyfunctionaris ingesteld. Uit het interview⁷¹ met de privacyfunctionaris blijkt dat zijn werkzaamheden onder andere bestaan uit het beantwoorden van vraagstukken die collega's stellen over privacy. Ook worden bij hem meldingen gedaan over het verwerken van persoonsgegevens als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens.

Op grond van artikel 63 lid 3 van de Wet bescherming persoonsgegevens dient een functionaris voor de gegevensbescherming aangemeld te worden bij het College bescherming persoonsgegevens. Uit voornoemd interview blijkt dat Avans niet heeft voldaan aan deze plicht. De privacyfunctionaris is derhalve niet terug te vinden in het openbaar register van functionarissen voor de gegevensbescherming. Er worden wel meldingen gedaan bij de privacyfunctionaris maar nu deze niet is aangemeld bij het College bescherming persoonsgegevens zijn deze melding niet geldig op grond van de Wet bescherming persoonsgegevens.

Aangezien Avans wel een privacyfunctionaris heeft aangesteld en klaarblijkelijk met het doel dat hij de taken uitvoert als bedoeld in de Wet bescherming persoonsgegevens dient Avans de privacyfunctionaris aan te melden bij het College bescherming persoonsgegevens.

4.5. CONCLUSIE

Er is nog geen social media richtlijn ingevoerd maar deze is in ontwikkeling. Om de social media richtlijn in overeenstemming te brengen met de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit is het raadzaam om een aantal regels toe te voegen aan de huidige regeling omtrent de controle op internet- en e-mailgebruik als bedoeld in paragraaf 2.5. van de huisregels. Om te waarborgen dat de inbreuk op de persoonlijke levenssfeer van werknemers minimaal blijft is het van belang dat wordt vastgelegd dat alleen berichten die op openbare delen van social media sites worden geplaatst zullen worden gecontroleerd. Om te voldoen aan het Vrijstellingsbesluit dienen de persoonsgegevens die zijn verkregen door controle van social media niet langer dan 6 maanden nadat zij zijn verkregen bewaard te worden. Tenslotte dient de ondernemingsraad in te stemmen met de gedragscode van social media wanneer het over het monitoren van social media gaat om in aanmerking te komen voor vrijstelling van de meldplicht als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens.

De huidige bewaartermijn van mobiele telefoniegegevens overschrijdt de bewaartermijn die het Vrijstellingsbesluit voorschrijft om vrijgesteld te worden van de meldplicht die de Wet bescherming persoonsgegevens voorschrijft. Om te voldoen aan het criterium van het Vrijstellingsbesluit dient de bewaartermijn van mobiele telefoniegegevens verlaagd te worden naar 6 maanden. Wanneer de bewaartermijn van de mobiele telefoniegegevens 6 maanden bedraagt, is Avans vrijgesteld van de meldplicht.

Wanneer de nieuwe HRM procedure ingevoerd wordt dient rekening te worden gehouden met verschillende bewaartermijnen voor de persoonsgegevens die ten behoeve van de

⁷¹ Zie bijlage 3.

personeelsadministratie verwerkt worden. Uitgangspunt is dat persoonsgegevens niet langer bewaard mogen worden dan nodig is voor het doel waarvoor de gegevens verwerkt zijn. Algemeen geldt een bewaartermijn van twee jaar nadat het dienstverband is beëindigd, tenzij een andere bewaartermijn geldt op basis van een wettelijke verplichting. De algemene Wet op de Rijksbelasting is van toepassing op alle werkgevers en noemt bewaartermijnen voor verschillende soorten persoonsgegevens. Daarnaast zijn er andere wetten die andere bewaartermijnen voorschrijven. Indien Avans zich aan de gestelde bewaartermijnen houdt dan is zij vrijgesteld van de meldplicht die de Wet bescherming persoonsgegevens oplegt.

Avans Hogeschool heeft een privacyfunctionaris aangesteld maar deze is niet aangemeld bij het College bescherming persoonsgegevens. Er worden bij hem wel meldingen gedaan over het verwerken van persoonsgegevens als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens. Om te voldoen aan de vereisten die de Wet bescherming persoonsgegevens noemt omtrent het aanstellen van een functionaris van de gegevensbescherming dient Avans de privacyfunctionaris aan te melden bij het College bescherming persoonsgegevens.

HOOFDSTUK 5

CONCLUSIES EN AANBEVELINGEN

Naar aanleiding van hetgeen dat in voorgaande hoofdstukken besproken is worden in dit hoofdstuk de conclusies omschreven. Aan de hand van de conclusies zullen daarna aanbevelingen worden gedaan.

5.1. CONCLUSIES

De controle op het e-mail en internetgebruik is zodanig geregeld dat de persoonlijke levenssfeer van medewerkers voldoende gewaarborgd is. De regeling voldoet aan de vereisten die de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit stellen. Doordat ook aan de vereisten van het Vrijstellingsbesluit is voldaan is de verwerking van voornoemde persoonsgegevens vrijgesteld van de meldplicht als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens. Avans hoeft hieromtrent geen nadere maatregelen te nemen.

Wanneer de social media richtlijn ingevoerd wordt zal deze aan dezelfde regels gebonden zijn als de regels die gelden voor het ICT-gebruik. Dat wil zeggen dat de controle daarop net als de controle op het e-mail en internetgebruik voldoet aan de vereisten van de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit. Omdat de regeling nog niet volledig is dient na de invoering van de definitieve regeling getoetst te worden of alle aspecten van die regeling ook voldoen aan het wettelijk kader.

Het cameratoezicht op Avans Hogeschool voldoet aan de noodzakelijkheidstoets van artikel 8 sub f van de Wet bescherming persoonsgegevens. Dat wil zeggen dat het belang van de werkgever in dit geval prevaleert boven het belang van de werknemer. De inbreuk op de persoonlijke levenssfeer is niet van zodanige aard dat er van cameratoezicht afgezien hoeft te worden. Tevens voldoet het cameratoezicht aan de vereisten van het Vrijstellingsbesluit omtrent cameratoezicht. Dus kan er worden geconstateerd dat Avans Hogeschool vrijgesteld is van de meldplicht als het gaat om cameratoezicht. Avans Hogeschool hoeft geen nadere maatregelen te nemen als het gaat over cameratoezicht om de regeling overeen te laten stemmen met de Wet bescherming persoonsgegevens.

De verwerking van telefoongegevens voldoet aan de vereisten van artikel 8 sub b van de Wet bescherming persoonsgegevens. De verwerking van vasttelefoniegegevens voldoet tevens aan de vereisten van het Vrijstellingsbesluit. De mobiele telefoniegegevens worden 24 maanden bewaard. Deze bewaartermijn overschrijdt de bewaartermijn die het Vrijstellingsbesluit voorschrijft. Tevens is de bewaartermijn niet noodzakelijk ter voldoening aan een wettelijke bewaarplicht. Dat wil zeggen dat de bewaartermijn van de mobiele telefoniegegevens te lang is en daardoor is Avans niet vrijgesteld van de meldplicht omtrent de verwerking van mobiele telefoniegegevens. Avans Hogeschool dient de bewaartermijn van mobiele telefoniegegevens te verlagen om de regeling overeen te laten stemmen met de Wet bescherming persoonsgegevens. Om te voldoen aan het transparantiebeginsel als bedoeld in artikel 33 en 34 van de Wet bescherming persoonsgegevens dient de regeling toegankelijk te zijn voor alle werknemers.

Tenslotte wordt binnenkort een nieuwe HRM procedure gestart die ervoor moet zorgen dat de personeelsadministratie voor een gedeelte door werknemers zelf of door

leidinggevend kan worden ingevoerd. Het privacyreglement persoonsgegevens personeel voldoet aan de vereisten die door de Wet bescherming persoonsgegevens worden gesteld aan de personeelsadministratie. Tevens voldoet de regeling aan het Vrijstellingsbesluit. Hieruit kan geconcludeerd worden dat de nieuwe HRM procedure is vrijgesteld van de meldplicht als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens.

Wanneer de nieuwe HRM procedure ingevoerd wordt dient rekening te worden gehouden met verschillende bewaartermijnen voor de persoonsgegevens die ten behoeve van de personeelsadministratie verwerkt worden. Uitgangspunt is dat persoonsgegevens niet langer bewaard mogen worden dan nodig is voor het doel waarvoor de gegevens verwerkt zijn. Algemeen geldt een bewaartermijn van twee jaar nadat het dienstverband is beëindigd, tenzij een andere bewaartermijn geldt op basis van een wettelijke verplichting. De algemene Wet op de Rijksbelasting is van toepassing op alle werkgevers en noemt bewaartermijnen voor verschillende soorten persoonsgegevens. Avans dient deze bewaartermijnen in acht te nemen om in overeenstemming met de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit te handelen.

Avans Hogeschool heeft een privacyfunctionaris aangesteld maar deze is niet aangemeld bij het College bescherming persoonsgegevens. Er worden bij hem wel meldingen gedaan over het verwerken van persoonsgegevens als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens. Om te voldoen aan de vereisten van de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit dient Avans de privacyfunctionaris aan te melden bij het College bescherming persoonsgegevens.

5.2. AANBEVELINGEN

Mobiele telefoniegegevens

De mobiele telefoniegegevens van werknemers worden momenteel 24 maanden bewaard. Deze bewaartermijn is niet in overeenstemming met de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit. Tevens rust er geen wettelijke verplichting op het zo lang bewaren van bovengenoemde gegevens. Om te voldoen aan de vereisten van de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit dient de bewaartermijn van mobiele telefoniegegevens verlaagd te worden naar 6 maanden. Als Avans besluit de bewaartermijn niet te verlagen dient er melding van de verwerking te worden gedaan bij het College bescherming persoonsgegevens of bij de functionaris van de gegevensbescherming.

Er dient een schriftelijke regeling te worden opgesteld met betrekking tot hoe lang de gegevens bewaard blijven en wie bevoegd is tot inzage van de gegevens om in overeenstemming met het transparantiebeginsel te handelen als bedoeld in artikel 33 en 34 van de Wet bescherming persoonsgegevens.

Social media richtlijn

Er is nog geen social media richtlijn ingevoerd maar deze is in ontwikkeling. Om de social media richtlijn in overeenstemming te brengen met de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit is het raadzaam om een aantal regels toe te voegen aan de huidige regeling omtrent de controle op internet- en e-mailgebruik als bedoeld in paragraaf 2.5. van de huisregels. Om te waarborgen dat de inbreuk op de persoonlijke levenssfeer van werknemers minimaal blijft is het van belang dat wordt vastgelegd dat alleen berichten die op openbare delen van social media sites worden geplaatst zullen worden gecontroleerd. Om te voldoen aan het Vrijstellingsbesluit dienen

de persoonsgegevens die zijn verkregen door controle van social media niet langer dan 6 maanden nadat zij zijn verkregen bewaard te worden. Tenslotte dient de ondernemingsraad in te stemmen met de gedragscode van social media wanneer het over het monitoren van social media gaat om in aanmerking te komen voor vrijstelling van de meldplicht als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens.

Nieuwe HRM procedure

Wanneer de nieuwe HRM procedure wordt ingevoerd dient Avans er zorg voor te dragen dat de wettelijke bewaartermijnen die voor personeelsadministratie gelden in acht worden genomen. In hoofdstuk 4 staat een tabel met de wettelijke bewaartermijnen voor verschillende soorten persoonsgegevens. Indien Avans zich aan die gestelde bewaartermijnen houdt dan is zij vrijgesteld van de meldplicht die de Wet bescherming persoonsgegevens oplegt.

Het privacyreglement personeel heeft onder andere als doelstelling voor de verwerking van persoonsgegevens: het (laten) uitvoeren van onderzoeken op het gebied van medewerkerstevredenheid, werkdruk onder werknemers of soortgelijke onderwerpen die voor de organisatie van belang zijn. Deze vorm van verwerking van persoonsgegevens wordt niet in de Wet bescherming persoonsgegevens of het Vrijstellingsbesluit genoemd. Om de persoonlijke levenssfeer van de werknemers te waarborgen en om in overeenstemming met de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit te handelen kan Avans ervoor kiezen om de onderzoeken anoniem uit te voeren. Op die manier worden er geen persoonsgegevens verwerkt en is de privacy voldoende gewaarborgd. Wanneer Avans ervoor kiest om de onderzoeken niet anoniem uit te voeren dient deze verwerking van persoonsgegevens gemeld te worden bij het College bescherming persoonsgegevens of bij de functionaris voor de gegevensbescherming.

Functionaris voor de gegevensbescherming

Tenslotte heeft Avans Hogeschool een privacyfunctionaris aangesteld welke niet is aangemeld bij het College bescherming persoonsgegevens. Toch worden bij hem wel meldingen gedaan omtrent gegevensverwerking als bedoeld in artikel 27 van de Wet bescherming persoonsgegevens. Om te voldoen aan de vereisten die de Wet bescherming persoonsgegevens noemt omtrent het aanstellen van een functionaris voor de gegevensbescherming dient Avans de privacyfunctionaris aan te melden bij het College bescherming persoonsgegevens. Indien Avans ervoor kiest de privacyfunctionaris niet aan te melden bij het College bescherming persoonsgegevens dienen meldingen omtrent de verwerking van persoonsgegevens gemeld te worden bij het College en niet bij de privacyfunctionaris.

HOOFDSTUK 6

EVALUATIE ONDERZOEK

In dit hoofdstuk wordt het verloop van het onderzoek geëvalueerd. Het onderzoeksresultaat geeft aan dat niet alle regelingen in overeenstemming met de Wet bescherming persoonsgegevens en het Vrijstellingsbesluit zijn. Om te beoordelen of de regelingen in overeenstemming met de wettelijke vereisten waren, was meer informatie nodig dan uitsluitend de regelingen zelf. Doordat niet alle informatie uit de regelingen gehaald kon worden werden interviews afgenomen met personen die over het desbetreffende onderwerp informatie konden verschaffen. De ervaring liet blijken dat de interviews best in een eerder stadium werden afgenomen om voldoende tijd te kunnen besteden aan het schrijven van de hoofdstukken. Tevens werd veel tijd besteed aan het schetsen van het juridisch kader om het onderwerp voldoende te beheersen. Hieruit voortvloeiend bleef er naar verhouding minder tijd over voor het analyseren van de regelingen.

Uiteindelijk zijn er aanbevelingen gedaan om trent het in overeenstemming brengen met huidige regelingen met actuele wet- en regelgeving. Uit het onderzoek bleek dat een aantal regelingen nog niet ingevoerd zijn maar dat er wel conceptregelingen zijn geschreven. Doordat er nog geen definitieve regelingen ingevoerd zijn kan slechts een aanbeveling worden gemaakt op basis van het concept en kan worden voorgesteld hoe de regeling geschreven moet worden om in overeenstemming te zijn met actuele wet- en regelgeving.

De onderzoeksresultaten geven aan dat een aantal regelingen aangepast dienen te worden. Tevens dienen een aantal regelingen ingevoerd te worden. Met deze resultaten blijkt dat het onderzoek een bijdrage heeft kunnen leveren aan de werkwijze van Avans Hogeschool omtrent de bescherming van de persoonlijke levenssfeer van werknemers.

LITERATUURLIJST

ELEKTRONISCHE BRONNEN

'Organisatie Avans Hogeschool', www.avans.nl, (zoek op: organisatie).

G. Overkleef-Verburg, 'De Grondwet, een systematisch en artikelsgewijs commentaar', Deventer, 2000.

Commissie Grondrechten in het digitale tijdperk, Rotterdam: Phoenix en Den Oudsten, 2000.

'Handreiking vrijstellingsbesluit', www.cbpweb.nl (zoek op handreiking vrijstellingsbesluit Wbp).

J.H.J. Terstegge, 'Goed werken in netwerken - regels voor controle ope-mailen internetgebruik van werknemers', Den Haag, 2002.

E. Thole en A. Engelfriet, 'Q&A over privacy, social media en de werkplek', ArbeidsRecht, 34, nr. 8/9, 2012.

CBP, 'Regels voor cameratoezicht', www.cbpweb.nl (zoek op: regels voor cameratoezicht).

CBP, 'Bewaartermijnen van persoonsgegevens in uw bestanden', informatieblad nr. 11a, juli 2012, www.cbpweb.nl.

Tuxx, 'Bewaartermijn personeelsdossier', www.tuxx.nl (zoek op bewaartermijn personeelsdossier).

LITERATUUR

G.A.F.M. Schaaijk, 'Praktijkgericht juridisch onderzoek', Den Haag: Boom juridische uitgevers 2011.

I. van der Helm, 'De privacybescherming van de zieke werknemer', Deventer: Kluwer, 2009.

D.J. Elzinga en R. De Lange, 'Het handboek van het Nederlandse staatsrecht', Deventer: Kluwer, 2006.

B.F. Keulen en G. Knigge, 'Kennismaking met het EVRM', Deventer: Kluwer, 2012.

H.H. De Vries en D.J. Rutgers, 'Wet bescherming persoonsgegevens toepassing in arbeidsverhoudingen', Deventer: Kluwer, 2001.

P.M.H.J. Van Grinsven, H.C. Geugjesen, H.N.M. Soemers, 'Arbeidsrecht begrepen', Den Haag: Boom juridische uitgevers, 2009.

JURISPRUDENTIE

ERHM 25 maart 1985, nr. NJ 1987,900 (Barthold/ Bondsrepubliek Duitsland).

EHRM 7 juli 1989, nr. NJ1991,659 (Gaskin/ Verenigd Koninkrijk).

EHRM 25 juni 1997, *LJN*: AD5858 (Halford/ Verenigd Koninkrijk).

HR 9 januari 1987, *LJN*: AG5500.

HR 8 oktober 2004, nr. C03/077HR.

Rb. Rotterdam 21 september 2011, nr.1263172.

Rb. Rotterdam 29 maart 2001, nr. AW 98/2443-LUG.

Rb. Arnhem, sector kanton, 19 maart 2012, *LJN* BV9483 (Blokker).

Rb. Arnhem, sector kanton Wageningen, 11 april 2012, *L/N* BW2006 (JK Vloerverwarming).

Ktr. Alkmaar 27 juni 2002, nr. 121750/02-1315.

EUROPESE RICHTLIJN

Richtlijn 95/46/EG (*PbEG* 1995 L 281/31).

KAMERSTUKKEN

Kamerstukken II 1997/1998, 25892, nr. 3, (MvT).

Kamerstukken II 2001/02, 5095178/01/6 (MvT).