

Controle op de werknemer

*De controle- en sanctiemogelijkheden
van de werkgever bij overmatig internetgebruik*



Auteur:	Sven van der Meer
Studentnummer:	2049952
Opdrachtgever:	Essent N.V.
Periode:	9 februari t/m 15 mei 2015
Opleiding:	HBO-Rechten
Afstudeermentor:	Mw. mr. M. van Dijk
Eerste afstudeerdocent:	Mw. mr. M.R.M. Brugman
Tweede afstudeerdocent:	Mw. mr. C.A.M. van der Voort
Plaats en datum:	's-Hertogenbosch, 28 mei 2015

Controle op de werknemer

De controle- en sanctiemogelijkheden
van de werkgever bij overmatig internetgebruik

Auteur:	Sven van der Meer
Functie auteur:	Afstuderend student
Studentnummer:	2049952
Opdrachtgever:	Essent N.V.
Opleiding:	HBO-Rechten, Juridische Hogeschool Avans-Fontys te 's-Hertogenbosch
Periode:	9 februari t/m 15 mei 2015
Afstudeermentor:	Mw. mr. M. van Dijk
Eerste afstudeerdocent:	Mw. mr. M.R.M. Brugman
Tweede afstudeerdocent:	Mw. mr. C.A.M. van der Voort
Plaats en datum:	's-Hertogenbosch, 28 mei 2015

Voorwoord

In het kader van mijn afstuderen aan de opleiding HBO-Rechten aan de Juridische Hogeschool Avans-Fontys te 's-Hertogenbosch, heb ik in opdracht van Essent een onderzoek uitgevoerd, waaruit dit onderzoeksrapport is voortgevloeid. De huidige technische ontwikkelingen en toenemende mogelijkheden op het internet, hebben het voor werknemers interessanter en makkelijker gemaakt om tijdens werktijd gebruik te maken van het internet. Omdat veel werknemers thuiswerken is het voor Essent steeds moeilijker om dit internetgebruik te controleren. Dit was voor Essent de aanleiding om een onderzoek uit te laten voeren naar de controlebevoegdheid en controlemogelijkheden die Essent heeft op het internetgebruik van werknemers. En of Essent bevoegd is zijn werknemers sancties op te leggen, indien er sprake is van overmatig internetgebruik en welke sanctiemogelijkheden Essent hiervoor heeft. Dit onderzoek is aan de hand van de toepasselijke wet- en regelgeving, jurisprudentie, vooraanstaande literatuur, rapportages, interne reglementen en interviews uitgevoerd. Hieruit vloeit een conclusie voort die antwoord geeft op de vraag of Essent zijn werknemers mag controleren op internetgebruik en bij overmatig internetgebruik mag sanctioneren.

Dit onderzoeksrapport is in de eerste plaats gericht aan mevrouw mr. M. van Dijk, die opdracht heeft gegeven voor dit onderzoek. Uiteraard is dit rapport ook gericht aan de afdeling Human Resources Management binnen Essent en de heer P. Buijs, die verantwoordelijk is voor de regelgeving betreffende de controle op internetgebruik.

Ik wil tot slot mijn stagebegeleider mevrouw mr. M. van Dijk en mijn eerste afstudeerdocent mevrouw mr. M.R.M. Brugman bedanken voor de begeleiding en steun die zij mij hebben geboden bij het maken van dit onderzoeksrapport. Ook de rest van mijn collega's van de afdeling Human Resources Management wil ik bedanken voor deze ondersteuning.

Voor nu wens ik u veel leesplezier toe.

Sven van der Meer

's-Hertogenbosch, mei 2015

Inhoudsopgave

Samenvatting

Lijst van afkortingen

Hoofdstuk 1 Inleiding	8
§ 1.1 Afstudeerorganisatie	8
§ 1.2 Aanleiding	8
§ 1.3 Doelstelling	9
§ 1.4 Vraagstelling	9
§ 1.5 Werkwijze en verantwoording	9
§ 1.6 Leeswijzer	10
§ 1.7 Beperkingen	10
Hoofdstuk 2 Theoretisch kader.....	11
§ 2.1 Inleiding	11
§ 2.2 Internet: geschiedenis en functioneren	11
§ 2.3 Definitie privacy	12
§ 2.4 Grondrechten: geschiedenis en definitie	12
§ 2.4.1 Verticale en horizontale werking grondrechten	13
§ 2.4.2 Europees Verdrag voor de Rechten van de Mens.....	13
§ 2.4.3 Europees Handvest van de Grondrechten van de Europese Unie	15
§ 2.4.4 Nederlandse Grondwet	16
§ 2.5 Wet bescherming persoonsgegevens	17
§ 2.5.1 College Bescherming Persoonsgegevens	18
§ 2.5.2 Reikwijdte	18
§ 2.5.2.1 Persoonsgegevens	19
§ 2.5.2.2 Verwerking van persoonsgegevens	20
§ 2.5.2.3 Geautomatiseerde of niet geautomatiseerde verwerking	20
§ 2.5.3 Verantwoordelijke en andere actoren.....	21
§ 2.5.4 Gewone en bijzondere persoonsgegevens	22
§ 2.5.5 Algemene beginselen verwerking persoonsgegevens	22
§ 2.5.5.1 Rechtmatigheid algemeen	22
§ 2.5.5.2 Doelbinding.....	22
§ 2.5.5.3 Rechtmatigheidsgronden	23
§ 2.5.5.4 Verenigbaar gebruik	25
§ 2.5.5.5 Kwaliteit en bewaartermijn	25
§ 2.5.5.6 Beveiliging en geheimhouding	26
§ 2.5.5.7 Meldplicht en voorafgaand onderzoek	26
§ 2.5.5.8 Rechten van betrokkenen	26
§ 2.6 Arbeidsrechtelijk kader	26
§ 2.6.1 Controlebevoegdheid.....	27
§ 2.6.2 Overmatig internetgebruik voor privédoeleinden	29
§ 2.6.3 Wet op de Ondernemingsraden	29
§ 2.6.4 Sanctiebevoegdheid	30
§ 2.6.4.1 Sanctie	30
§ 2.6.4.2 Soorten sancties	31
§ 2.6.4.3 Straf of ordemaatregel	31
§ 2.6.4.4 Sanctiebeginselen	32
§ 2.6.4.5 Jurisprudentie sancties	32
§ 2.7 Toekomstige veranderingen in het recht op privacy	33
§ 2.8 Samenvatting.....	35

Hoofdstuk 3 Praktijk Essent.....	36
§ 3.1 Inleiding	36
§ 3.2 Arbeidsovereenkomst	36
§ 3.3 Bedrijfsmiddelen	36
§ 3.4 Thuiswerken	36
§ 3.5 Internet- en controlebeleid	37
§ 3.5.1 Overmatig internetgebruik voor privédoeleinden	37
§ 3.5.2 Controle op internetgebruik.....	37
§ 3.5.3 Beveiliging van persoonsgegevens.....	39
§ 3.6 Sancties.....	40
§ 3.7 Samenvatting.....	41
Hoofdstuk 4 Toepassing recht op praktijk Essent	42
§ 4.1 Inleiding	42
§ 4.2 Controlebevoegdheid.....	42
§ 4.3 Controlemogelijkheden en de Wbp	42
§ 4.3.1 Toetsing aan reikwijdte Wbp.....	43
§ 4.3.2 Toepassing Wbp.....	44
§ 4.4 Controle bij BYOD en thuiswerken.....	47
§ 4.5 Sanctiemogelijkheden.....	48
§ 4.6 Samenvatting.....	49
Hoofdstuk 5 Conclusies en aanbevelingen.....	50
§ 5.1 Inleiding	50
§ 5.2 Conclusies	50
§ 5.3 Aanbevelingen.....	52
Literatuurlijst/bronvermelding	53

Samenvatting

De huidige technologische ontwikkelingen hebben ervoor gezorgd dat er steeds meer mogelijkheden zijn voor het gebruik van internet. Een neveneffect van deze ontwikkelingen is dat werknemers makkelijker en sneller worden afgeleid van hun werk. Dit kan voor bedrijven een aanleiding zijn om het internetgebruik van werknemers te controleren. De werkgever wordt hierin echter bemoeilijkt, doordat de werknemer zijn werkzaamheden steeds vaker thuis uitvoert. Deze ontwikkelingen waren voor Essent de aanleiding om een onderzoek uit te laten voeren naar de controlebevoegdheid en controlemogelijkheden die Essent heeft op het internetgebruik van werknemers. En of Essent bevoegd is zijn werknemers sancties op te leggen, indien er sprake is van overmatig internetgebruik en welke sanctiemogelijkheden Essent hiervoor heeft. Met dit rapport wordt beoogd om op 1 juni 2015 een advies uit te brengen aan de afdeling Human Resources Management van Essent, waarin de volgende centrale vraag wordt beantwoord: 'In hoeverre mag Essent zijn werknemers, gelet op de huidige wet- en regelgeving en de privacyregels van Essent, controleren op overmatig internetgebruik en bij overtreding daarvan sanctioneren?'. Om tot een valide conclusie te komen heeft er een desk-research plaatsgevonden. Aan de hand van dit onderzoek heeft er een inhoudsanalyse naar de geldende internationale, Europese en nationale wet- en regelgeving plaatsgevonden. Daarvoor is jurisprudentie, vooraanstaande literatuur, rapportages en andere (digitale) documenten op inhoud geanalyseerd.

Werknemers hebben op grond van artikel 8 EVRM en artikel 10 Gw het recht op privacy. Het recht op privacy geldt niet alleen op de werkplek op kantoor, maar ook op de werkplek thuis en de communicatie via het internet. In beginsel mag de werkgever hier geen inbreuk op maken. Rechtmatige beperking is mogelijk, wanneer wordt voldaan aan artikel 8 EVRM, artikel 10 Gw of de Wbp.

Essent is op grond van de wettelijke instructiebevoegdheid (artikel 7:660 BW), het goed werknemerschap (artikel 7:611 BW), in combinatie met de contractuele vertrouwensrelatie tussen Essent en de werknemer, bevoegd om zijn werknemers bij een vermoeden dat regels worden overtreden te controleren. Zo ook bij een vermoeden van overmatig internetgebruik voor privédoeleinden. In jurisprudentie is bepaald dat er sprake is van overmatig internetgebruik voor privédoeleinden, wanneer aan het internetgebruik buitenproportioneel veel tijd wordt besteed of dit gebruik ernstig ten koste gaat van de werkzaamheden.

Bij een vermoeden dat een werknemer overmatig gebruik maakt van het internet voor privédoeleinden, is Essent bevoegd te controleren op getotaliseerde gegevens waaruit identificatie van een persoon (redelijkerwijs) onmogelijk is. Wanneer een werknemer wordt verdacht overmatig gebruik te maken van het internet voor privédoeleinden, kan Essent gericht op het internetgebruik van deze werknemer controleren. Deze controle dient in beginsel alleen op verkeersgegevens plaats te vinden. Een controle op inhoud is door de ontbrekende zwaarwegende redenen van Essent in beginsel niet mogelijk.

In beginsel worden werknemers bij een gerichte controle op internetgebruik voorafgaand aan de controle door Essent op de hoogte gesteld van de identiteit van Essent en het doel van de controle. Dit wordt een open onderzoek genoemd. De andere mogelijkheid is de heimelijke controle, waarbij de werknemer niet voorafgaand aan de controle op de hoogte wordt gesteld. Voor deze controle dient er een "zwaarwegend belang" aanwezig te zijn, die in de meeste situaties bij overmatig internetgebruik niet aanwezig is. De controles op internetgebruik mogen door Essent alleen op werknemers die op kantoor aanwezig zijn worden uitgevoerd. Wanneer uit de controle is gebleken dat er sprake is van overmatig internetgebruik voor privédoeleinden, dan is Essent op grond van het arbeidsrecht bevoegd tot het opleggen van sancties. Deze sancties zijn gebaseerd op het arbeidsrecht en de CAO PLb. Bij het inzetten van deze sancties dient rekening te worden gehouden met sanctiebeginselen uit het arbeidsrecht, de CAO PLb en de toepasselijke jurisprudentie.

Lijst van afkortingen

art.	Artikel
AVG	Algemene verordening gegevensbescherming
BW	Burgerlijk Wetboek
CAO	Collectieve arbeidsovereenkomst
CAO PLb	CAO Productie- en Leveringsbedrijven
CBP	College Bescherming Persoonsgegevens
CBS	Centraal Bureau voor de Statistiek
COR	Centrale Ondernemingsraad
EG	Europese Gemeenschap
EHRM	Europees Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
Gw	Grondwet
Handvest	Handvest van de grondrechten van de Europese Unie
HR	Hoge Raad
HvJ EG	Hof van Justitie van de Europese Gemeenschappen (<i>bij uitspraken tot 1 december 2009</i>)
HvJ EU	Hof van Justitie van de Europese Unie
IVBPR	Internationaal verdrag inzake burgerrechten en politieke rechten
jo.	Juncto
ktr.	Kantonrechter
MvT	Memorie van toelichting
N.V.	Naamloze Vennootschap
OR	Ondernemingsraad
Rb.	Rechtbank
SMTP	Simple Mail Transfer Protocol
Stb.	Staatsblad
TCP/IP	Transmission Control Protocol/Internet Protocol
Trb.	Tractatenblad
UVRM	Universele Verklaring van de Rechten van de Mens
VN	Verenigde Naties
VWEU	Verdrag betreffende de werking van de Europese Unie
Wbp	Wet bescherming persoonsgegevens
WOR	Wet op de Ondernemingsraden

Hoofdstuk 1 Inleiding

Dit hoofdstuk geeft een inleiding in het praktijkgericht onderzoek dat voor Essent N.V. wordt verricht. De inleiding begint met een beschrijving van de afstudeerorganisatie. Vervolgens wordt de aanleiding voor dit onderzoek, de doelstelling en vraagstelling beschreven. Daaropvolgend komen de methode van onderzoek, de verantwoording, de opbouw van dit rapport en de beperkingen aan bod.

§ 1.1 Afstudeerorganisatie

De organisatie waarvoor dit afstudeeronderzoek is verricht, is het energiebedrijf Essent N.V. (hierna: Essent) dat gas, elektriciteit en energiediensten aan 2,5 miljoen consumenten en bedrijven in Nederland en België levert. Essent is sinds 2009 100% onderdeel van het Duitse RWE, dat één van Europa's belangrijkste internationale energieconcerns is.¹ Eind 2013 werkten er 3.115 mensen bij Essent (inclusief RWE Generation Nederland).

Dit afstudeeronderzoek zal bij Essent Nederland in 's-Hertogenbosch worden uitgevoerd en zich daarmee ook alleen richten op Essent Nederland.²

§ 1.2 Aanleiding

Privacy is tegenwoordig een 'hot item'. In het nieuws wordt regelmatig de aandacht gevestigd op de verwerking en beveiliging van (persoons)gegevens door verschillende grote bedrijven, zoals Facebook³ en Google⁴. Omdat personen in Europa, dus ook in Nederland, het recht hebben op eerbiediging van de persoonlijke levenssfeer, het privéleven en correspondentie⁵, zijn er regels vastgelegd die de privacy moeten beschermen. Deze wettelijke regels vloeien voort uit verdragen en Europese Richtlijnen, waaruit privacywetgeving, de Wet bescherming persoonsgegevens, tot stand is gekomen.⁶ Deze regels zijn niet alleen van belang voor commerciële bedrijven die klantgegevens verwerken, maar ook voor werkgevers.

In deze moderne wereld wordt er van werknemers steeds meer flexibiliteit verwacht, waardoor er vaker (gedeeltelijk) wordt thuis gewerkt.⁷ Om deze flexibiliteit mogelijk te maken stellen veel werkgevers een computer en/of smartphone aan werknemers ter beschikking. Door deze trend worden werktijden flexibeler, hebben werknemers de mogelijkheid om thuis te werken en zijn werk en privé steeds moeilijker van elkaar te scheiden. Het wordt voor de werkgever bij thuiswerkende werknemers moeilijker om deze werknemers te controleren, dan dat dit in de oude situatie was, waar werknemers elkaar op de werkvloer "controleren". Daarnaast blijven de mogelijkheden op het internet en het internetgebruik alsmaar toenemen. Voor werknemers is het daardoor steeds interessanter om tijdens werktijd gebruik te maken van het internet voor privédoeleinden.⁸ Zo is het tegenwoordig gebruikelijk om via social media contact te houden met het thuisfront of vrienden, nieuwsberichten te lezen of online te winkelen. Deze ontwikkelingen zorgen er volgens veel werkgevers voor dat werknemers afgeleid raken in hun dagelijkse werkzaamheden, waardoor in sommige gevallen het werk hieronder te leiden heeft.⁹

¹ 'Over RWE', Essent, www.essent.nl (zoek op *RWE*) (laatst geraadpleegd op 31 maart 2015).

² 'Profiel', Essent, www.essent.nl (zoek op *profiel Essent*) (laatst geraadpleegd op 31 maart 2015).

³ 'CBP onderzoekt nieuwe privacyvoorwaarden Facebook', CBP, www.cbp.nl (zoek op *privacyvoorwaarden Facebook*) (laatst geraadpleegd op 31 maart 2015).

⁴ 'CBP legt Google sanctie op voor privacyschendende voorwaarden', CBP, www.cbp.nl (zoek op *privacy Google*) (laatst geraadpleegd op 31 maart 2015).

⁵ art. 8 EVRM jo. 10 Gw.

⁶ Richtlijn 95/46/EG (*PbEG* 1995 L 281/31); art. 1 sub a jo. sub b jo. art. 2 lid 1 Wbp.

⁷ Rapport CBS ICT kennis en economie 2014, p. 13.

⁸ Rapport TNS NIPO Media Standaard Survey 2013, p. 7.

⁹ Dancet e.a. 2013, p. 65.

In het verleden heeft Essent op de technische en privacyontwikkelingen proberen in te spelen. Dit heeft zich in 2002 vertaald in een ICT-reglement, waardoor het onder bepaalde vereisten mogelijk is om controles uit te voeren op het ICT-gebruik van werknemers.¹⁰

De huidige technische ontwikkelingen en toenemende mogelijkheden op het internet, hebben het voor werknemers interessanter en makkelijker gemaakt om tijdens werktijd gebruik te maken van het internet. Omdat veel werknemers thuiswerken is het voor Essent steeds moeilijker om dit internetgebruik te controleren. Dit was voor Essent de aanleiding om een onderzoek uit te laten voeren naar de controlebevoegdheid en controlemogelijkheden die Essent heeft op het internetgebruik van werknemers. En of Essent bevoegd is zijn werknemers sancties op te leggen, indien er sprake is van overmatig internetgebruik en welke sanctiemogelijkheden Essent hiervoor heeft. Tevens is het reglement dat toeziet op ICT-gebruik meer dan tien jaar oud. Om die reden is het voor Essent van belang om de punten met betrekking tot de controle op het internet gebruik uit dit reglement juridisch te onderwerpen aan een juridische herbeoordeling.

§ 1.3 Doelstelling

Met dit rapport wordt beoogd om op 1 juni 2015 een advies uit te brengen aan de afdeling Human Resources Management van Essent, waaruit blijkt óf en zo ja onder welke voorwaarden Essent conform de geldende wet- en regelgeving en de privacyreglementen binnen Essent werknemers op internetgebruik mag controleren en sanctioneren.

§ 1.4 Vraagstelling

De centrale vraag die de basis vormt voor dit onderzoek luidt als volgt:

‘In hoeverre mag Essent zijn werknemers, gelet op de huidige wet- en regelgeving en de privacyregels van Essent, controleren op overmatig internetgebruik en bij overtreding daarvan sanctioneren?’

Deze centrale vraag is opgedeeld in een aantal deelvragen. De deelvragen zien er als volgt uit:

- 1) Welke wet- en regelgeving is van toepassing op controle op internetgebruik van werknemers?
- 2) Is het voor Essent als werkgever, op grond van de wet- en regelgeving en de privacyregels van Essent, toegestaan om zijn werknemers op het internetgebruik te controleren?
- 3) Wanneer is er op grond van de wet- en regelgeving en Essent sprake van overmatig internetgebruik?
- 4) Is Essent als werkgever, op grond van de wet- en regelgeving en regels binnen Essent, bevoegd om sancties op te leggen en welke sancties kunnen er bij overmatig internetgebruik worden opgelegd?

§ 1.5 Werkwijze en verantwoording

Om tot een valide conclusie te komen op de centrale vraag uit dit rapport, heeft er een desk-research plaatsgevonden. Aan de hand van dit onderzoek heeft er eerst inhoudsanalyse van de geldende internationale, Europese en nationale wet- en regelgeving plaatsgevonden. Daarvoor is jurisprudentie, vooraanstaande literatuur, rapportages en andere (digitale) documenten op inhoud geanalyseerd. Vervolgens zijn de reglementen, regelingen en overeenkomsten die op Essent van toepassing zijn op inhoud geanalyseerd en hebben er interviews plaatsgevonden. Voor de bovenstaande methode is gekozen, omdat het gebruik van deze bronnen en de manier van onderzoeken zal leiden tot een valide onderzoeksresultaat.

¹⁰ Zie bijlage 3 ‘Reglement Essent Controle op het ICT-gebruik’; Zie bijlage 4 ‘Concernregeling Privacyreglement Essent’.

§ 1.6 Leeswijzer

Dit rapport bestaat uit vijf hoofdstukken en is onderverdeeld in (sub)paragrafen. In hoofdstuk twee wordt het theoretisch kader uiteengezet. In dit hoofdstuk komt informatie over het internet, de privacy, de internationale en nationale privacygrondrechten, de Wet bescherming persoonsgegevens, het arbeidsrechtelijke kader omtrent het controleren van werknemers, het overmatig internetgebruik, de sanctiebevoegdheid van de werkgever en de toekomstige Europese privacyverordening aan bod.

In hoofdstuk drie wordt de praktijk omtrent de controle op internetgebruik uiteengezet. In dit hoofdstuk komt de arbeidsovereenkomst, de bedrijfsmiddelen, het thuiswerken, het internet- en controlebeleid en de sancties aan bod.

In hoofdstuk vier wordt het recht uit hoofdstuk twee op de praktijk van Essent uit hoofdstuk drie toegepast. Als eerste wordt gekeken naar de controlebevoegdheid van Essent. Vervolgens worden de controlemogelijkheden van Essent op de wet- en regelgeving toegepast, de controle bij thuiswerken en BYOD en komen de sanctiemogelijkheden van Essent aan bod. Tot slot zullen in hoofdstuk vijf de conclusies en aanbevelingen worden gegeven.

§ 1.7 Beperkingen

Helaas is het na verschillende pogingen niet gelukt om de netwerkbeheerder van Essent voor dit onderzoeksrapport te interviewen.

Hoofdstuk 2 Theoretisch kader

§ 2.1 Inleiding

In dit hoofdstuk wordt het theoretisch kader omtrent het controleren en sanctioneren van werknemers op internetgebruik uiteengezet. In de tweede paragraaf wordt de geschiedenis en het functioneren van het internet beschreven. De derde paragraaf beschrijft de geschiedenis en de definitie van het begrip privacy. Vervolgens wordt in de vierde paragraaf de geschiedenis en definitie van internationale grondrechten beschreven. Aansluitend wordt in de subparagrafen de verticale en horizontale werking van grondrechten uiteengezet en komen de internationale, Europese en nationale grondrechten op privacy aan bod. In de daaropvolgende paragraaf en subparagrafen komt de Wet bescherming persoonsgegevens aan bod en wordt deze wet uiteengezet. Vervolgens wordt in paragraaf zes en de subparagrafen het arbeidsrechtelijke kader uiteengezet, waarin de controlebevoegdheid, het overmatig internetgebruik voor privédoeleinden, de Wet op de Ondernemingsraden en de sanctiebevoegdheid uiteen worden gezet. Tot slot komt de toekomstige Europese verordening op het gebied van de verwerking van persoonsgegevens aan bod.

§ 2.2 Internet: geschiedenis en functioneren

Het internet bestaat al meer dan veertig jaar en is sinds 1993 opengesteld voor publiek. Sinds die tijd is het een wereldomspannend publieknetwerk, dat uit verschillende netwerken bestaat.¹¹ Het internet heeft een verscheidenheid aan verschijningsvormen, die in de basis allemaal gebruikmaken van het TCP/IP-protocol¹². Ieder apparaat dat met een intern netwerk (zoals een bedrijfsnetwerk) of het internet verbonden is, heeft op basis van dit protocol een uniek IP-adres. Dit adres is in feite vergelijkbaar met een huisadres, waarmee je jezelf identificeert.¹³ Aan de hand van het soort internetgebruik wordt het daarbij behorende protocol bepaald en gebruikt. Bij het bezoeken van bijvoorbeeld een internetwebsite op het World Wide Web (WWW), wordt er gebruikgemaakt van HTTP-protocol¹⁴ en bij het versturen van e-mailberichten het SMTP-protocol¹⁵. Als voorbeeld zal het bezoeken van een internetwebsite op het WWW worden genomen. Bij het aanvragen van een internetwebsite, wordt de aanvraag in verschillende pakketjes geknipt, waar het TCP/IP-protocol aan ieder pakketje een code koppelt. In deze code staat ondermeer het afzendadres en het bestemmingadres, zodat de pakketten bij het juiste apparaat aankomen en het aangevraagde bij het juiste apparaat wordt afgeleverd. Door deze code weet ieder apparaat dat op de route tussen de aanvrager en bron ligt voor wie dit pakket bestemd is.¹⁶ Binnen veel bedrijfsnetwerken loopt de toegang naar het internet vaak via een centrale schakel die een server heet. Doordat al het verkeer via deze server loopt, kan al het dataverkeer tussen de computer en het internet door bijvoorbeeld software op de server gecontroleerd en/of geregistreerd worden.¹⁷ Dit wordt ook wel “loggen” of “logging” genoemd, dat het bijhouden van gegevens over het gebruik van (computer)systemen en/of programma's inhoudt.¹⁸ Een voorbeeld waarop communicatie kan verlopen is hieronder in afbeelding 1 te zien. In werkelijkheid kan de communicatie op een meer ingewikkelde manier plaatsvinden, maar dat voert hier te ver.

¹¹ Hof e.a. 2014, p. 1.

¹² Transmission Control Protocol (TCP) en Internet Protocol (IP).

¹³ Vries, Van der Jagt & Roosendaal 2008, p. 1.

¹⁴ Hypertext Transfer Protocol.

¹⁵ Simple Mail Transfer Protocol.

¹⁶ Hof e.a. 2014, p. 1-3; Terstegge 2002, p. 12-14 en 17.

¹⁷ Vries, Van der Jagt & Roosendaal 2008, p. 1.

¹⁸ Terstegge 2002, p. 13.



Afbeelding 1 - Voorbeeld verloop van communicatie bij het raadplegen van een internetwebsite.

§ 2.3 Definitie privacy

Het begrip 'privacy' vindt zijn oorsprong in de Verenigde Staten. De jurist Brandeis zette dit begrip in 1890, met als definitie "the right to be left alone", op de agenda. Met dit begrip wees hij er voornamelijk op dat privacy van essentieel belang is voor de bescherming van de persoonlijkheid, de onafhankelijkheid, de waardigheid en integriteit van het individu.¹⁹ Privacy wordt nu vaak omschreven als een dubbelzinnig, dynamisch en ondefinieerbaar begrip. Dit komt volgens mr. P.H. Blok onder andere doordat in de praktijk met de privacy niet als absoluut recht wordt omgegaan, maar hierbij juist naar de rechtvaardiging van de beperking hierop wordt gekeken. Daarnaast is het begrip privacy een breed begrip dat op verschillende situaties van toepassing kan zijn, zoals bescherming tegen ongerechtvaardigde verwerking van persoonsgegevens, de lichamelijke privacy en de ruimtelijke privacy. Dit onderzoek richt zich op de privacy van werknemers bij de controle op het internetgebruik (informationele privacy) dat de aanspraken van het individu op bescherming en verwerking van persoonsgegevens inhoudt. De informationele privacy is voor dit rapport van groot belang en zal in dit rapport worden uitgewerkt.²⁰

§ 2.4 Grondrechten: geschiedenis en definitie

Grondrechten, die ook wel fundamentele rechten of mensenrechten worden genoemd, zijn rechten die inherent zijn aan het mens-zijn en die de grenzen van het legitiem handelen van de overheid bepalen.²¹ De geschiedenis van grondrechten begon vlak na het einde van de Tweede Wereldoorlog. Na deze oorlog, waarin veel grondrechten werden geschonden, was in de wereld de overtuiging dat een betere, volwaardige bescherming van grondrechten noodzakelijk zou zijn voor behoud van vrede en veiligheid. Dit heeft zich vertaald in de grondrechtverdragen die in 1950 door de Verenigde Naties (hierna: VN) in de vorm de Universele Verklaring van de Rechten van de Mensen (hierna: UVRM) en door de Raad van Europa²² in de vorm van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM) zijn opgesteld. Beide documenten bevatten een artikel dat betrekking heeft op het recht op respect van onder andere het privé leven, briefwisseling en correspondentie.²³ Omdat het UVRM niet juridisch bindend is, heeft de VN in 1969 het Internationaal verdrag inzake burgerrechten en politieke rechten (hierna: IVBPR) uitgevaardigd. Aangezien het IVBPR en het EVRM beide het recht op privacy beschermen en het EVRM in de Nederlandse samenleving een grotere rol speelt, wordt het IVBPR, ondanks zijn belangrijke betekenis, in dit rapport verder buiten beschouwing gelaten.²⁴

¹⁹ Borking 2010, p. 21.

²⁰ Berkvens e.a. 2007, p. 5 en 7-8 en 186; HR 31 mei 2002, ECLI:NL:PHR:2002:AD9609, (concl. A-G Stikwerda punt 24).

²¹ Henrard 2006, p. 27 en 29.

²² Henrard 2006, p. 100-101: De Raad van Europa is een internationale organisatie, dat een bijzondere focus heeft op mensenrechten en niet verward mag worden met de Europese Unie.

²³ Henrard 2006, p. 57, 100-101; Berkvens e.a. 2007, p. 9; art. 12 UVRM en 8 EVRM; Terstegge 2002, p. 19.

²⁴ Berkvens e.a. 2007, p. 10; art. 17 IVBPR en 8 EVRM.

§ 2.4.1 Verticale en horizontale werking grondrechten

Voordat er op het EVRM en andere grondrechten wordt ingegaan, is het van belang om aan te geven wie op deze grondrechten een beroep kunnen doen.

Grondrechten worden oorspronkelijk begrepen als een bescherming voor particulieren (ook burgers genoemd) in verhouding tot de overheid. Dit wordt de verticale werking genoemd. Deze verticale werking impliceert meer dan alleen de onthoudingsplicht (verbod op inmenging) van de overheid, namelijk ook de positieve verplichting om grondrechten te waarborgen in relaties tussen particulieren. De relatie tussen particulieren, zoals een werknemer tegen de werkgever wordt de horizontale werking genoemd.²⁵ Deze horizontale werking is van belang voor dit onderzoek. In de literatuur spreekt men over directe horizontale werking aan de ene kant en indirecte horizontale werking aan de andere kant. De indirecte horizontale werking houdt in dat een particulier een klacht tegen een Staat indient, waarin hij aangeeft dat de Staat niet heeft voldaan aan zijn positieve verplichting. Wanneer particulieren deze grondrechten tegenover elkaar, ten overstaan van de nationale rechter, invoeren, dan is er sprake van een directe horizontale werking.²⁶ In de navolgende paragrafen wordt per grondrechtelijk artikel aangegeven of er sprake is van een (directe of indirecte) horizontale werking.

2.4.2 Europees Verdrag voor de Rechten van de Mens

Het EVRM, dat in paragraaf 2.4 al aan bod kwam, is sinds de ratificering door Nederland in 1954 juridisch bindend.²⁷ Door deze ratificering, ook wel bekrachtiging genoemd, is de Nederlandse Staat en de overheden van de Nederlandse Staat, gehouden om dit verdrag te respecteren tegenover haar burgers (verticale werking).²⁸ Daarnaast is het verdedigbaar dat dit artikel, ondanks de controverse in de literatuur, niet alleen een verticale werking, maar ook een (directe) horizontale werking heeft.²⁹ Doordat uit de formulering van het toepasselijke artikel 8 EVRM, dat onder andere ziet op het recht van respect voor privé leven en correspondentie, blijkt dat het 'een ieder' verbindt heeft dit artikel een directe werking.³⁰ In 1987 heeft de Hoge Raad erkend dat dit grondrecht ook tussen particulieren onderling geldt, zodat dit recht een directe horizontale werking heeft.³¹ Tevens heeft de Hoge Raad³² in 2001, in navolging van verschillende rechtbanken, de doorwerking van artikel 8 EVRM in arbeidsverhoudingen aanvaard.³³ Ondanks de controverse die in de literatuur bestaat, kunnen particulieren zich op grond van de directe horizontale werking beroepen.

Artikel 8 EVRM ziet er als volgt uit:

‘1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economische welzijn van het land, het voorkomen van

²⁵ Henrard 2006, p. 9 en 50.

²⁶ Henrard 2006, p. 51.

²⁷ ‘Verdragen en wetten’, College voor de rechten van de mens, www.mensenrechten.nl (zoek op *ratificeren EVRM*) (laatst geraadpleegd op 23 april 2015); art. 17 IVBPR.

²⁸ Henrard 2006, p. 27, Kooijmans 2008, p. 96-98.

²⁹ Helm 2009, p. 38.

³⁰ art. 93 jo. 94 Gw.

³¹ HR 9 januari 1987, ECLI:NL:HR:1987:AG5500, r.o. 4.4.

³² HR 27 april 2001, ECLI:NL:HR:2001:AB1347, r.o. 3.7.

³³ Berkvens e.a. 2007, p. 186.

*wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.’*³⁴

Aan de hand van dit artikel is er in de loop der jaren door het bevoegde gerechtshof, het Europese Hof voor de Rechten van de Mens (hierna: EHRM), belangrijke jurisprudentie gewezen. De belangrijkste punten die hieruit voortvloeien en die van belang zijn voor dit rapport worden hieronder per zaak beschreven.

Niemietz tegen Bondsrepubliek Duitsland

Het EHRM heeft in de zaak Niemietz tegen de Bondsrepubliek Duitsland bepaald dat het recht op privacy, dat onder andere ziet op het privéleven uit artikel 8 EVRM, zich ook uitstrekt tot de zakelijke activiteiten en de ruimten van een individu. Het EHRM bepaalde dat het recht op privacy van de werknemer langs drie wegen kan worden vastgesteld:

- I. Een groot deel van het individuele leven speelt zich op het werk af, waardoor een goed onderscheid tussen privéleven en het zakelijke leven niet te maken is;
- II. er is geen onderscheid te maken tussen privé- en zakelijke communicatie; en
- III. zakelijke activiteiten kunnen zowel op een thuisadres als kantooradres worden ontplooid, denk aan thuiswerken.³⁵

Halford tegen Verenigd Koninkrijk

Nadat in de zaak Niemietz bepaald is dat voor werknemers het recht op privacy ook geldt, werd er in het arrest Halford tegen Verenigd Koninkrijk door het EHRM geoordeeld dat het recht op privacy zich (tot op zekere hoogte) ook uitstrekt tot de werkplek. Belangrijk in deze uitspraak is dat het EHRM aangaf dat het recht op correspondentie uit artikel 8 EVRM, zich mede uitstrekt tot telefoongesprekken die vanaf zowel een werkplek als thuis worden gevoerd. Doordat in deze zaak de werkgever zijn werknemer er nooit op had gewezen dat de mogelijkheid bestond dat de communicatiesystemen zou worden gecontroleerd, had de werknemer volgens het EHRM een “redelijke verwachting tot privacy”.³⁶ Het bekend zijn met de mogelijkheid op controle is dus een basisvoorwaarde voor de rechtmatigheid ervan.

Copland tegen Verenigd Koninkrijk

Vervolgens is in een recenter arrest, het arrest Copland tegen Verenigd Koninkrijk, door het EHRM geoordeeld dat het recht op privacy op de werkplek ook voor elektronische communicaties bestaat, ongeacht of deze een privé of zakelijk karakter hebben. Onder deze communicatie worden niet alleen telefoongesprekken verstaan, maar ook e-mailberichten en informatie die voortvloeit uit het monitoren van internetgebruik. Hierbij gaat het niet alleen om de inhoud van de communicatie, maar ook de verkeersgegevens, zoals de contactpersoon en waarvandaan de communicatie plaatsvond. Het EHRM merkt op dat het begrip ‘privé correspondentie’ uit artikel 8 lid 1 EVRM ‘dynamisch uitgelegd’ moet worden, inhoudende dat dit begrip aan de hand van de stand van de techniek van dat moment dient te worden uitgelegd. Daarbij merkt het EHRM wel op dat controle van telefoon, e-mail en internetgebruik slechts onder bepaalde omstandigheden is toegestaan. Welke omstandigheden wordt niet toegelicht, wel dient er een wettelijke basis te zijn voordat een werknemer gecontroleerd mag worden.³⁷

Samengevat kan er aan de hand van de bovenstaande jurisprudentie, die betrekking heeft op artikel 8 EVRM, het volgende worden geconcludeerd:

- een werknemer heeft het recht op privacy;

³⁴ Trb. 1951, 154, p. 8; ‘Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden’, Nederlandse overheid, overheid.nl (zoek op EVRM) (laatst geraadpleegd op 23 april 2015).

³⁵ EHRM 16 december 1992, NJ 1993, 400, m.nt. E.J. Dommering (*Niemietz/Bondsrepubliek Duitsland*).

³⁶ EHRM 25 juni 1997, 173/1996, NJ 1998, 506, m.nt. P.J. Boon (*Halford/Verenigd Koninkrijk*).

³⁷ EHRM 3 april 2007, 62617/00, NJ 2007, 617, m.nt. E.J. Dommering (*Copland/Verenigd Koninkrijk*).

- het recht op privacy geldt op de werkplek, dit kan zowel thuis als op kantoor zijn;
- het recht op privacy zowel voor privé- als voor zakelijke communicatie bestaat;
- het begrip 'communicatie' dient uitgelegd te worden naar de stand van de techniek, waar zeker e-mail-, telefoon- en internetverkeer onder vallen en niet alleen de inhoud (het gesprek of tekst) van de communicatie, maar ook de verkeersgegevens;
- in het geval de werkgever zijn werknemers wil controleren op communicatie dient hij zijn werknemers hiervan vooraf op de hoogte te stellen, zodat de werknemers geen "redelijke verwachting tot privacy" hebben.

Op grond van de bovengenoemde jurisprudentie blijkt dat werknemers het recht hebben op privacy, maar dit betekent niet dat dit recht absoluut is. Op grond van artikel 8 lid 2 EVRM kan de werkgever dit recht beperken, wanneer er aan de in het lid 2 genoemde vereisten wordt voldaan. Wanneer aan deze vereisten voor beperking is voldaan, is er sprake van een rechtmatige inbreuk op de privacy. Indien er niet aan de vereisten is voldaan, is er sprake van schending van het recht op privacy.³⁸

In artikel 8 lid 2 EVRM staat dat alleen 'inmenging van enig openbaar gezag' is toegestaan. Dit vormt volgens het EHRM³⁹ en de Hoge Raad⁴⁰ geen beletsel om dit lid in een directe horizontale verhouding tussen werknemer en werkgever toe te passen. De toetsing aan de vereisten dient tussen de werkgever en werknemer gelijk te zijn met die van de toetsing tussen de overheid en particulier.⁴¹ Voor deze rechtvaardiging dient er aan een viertal vereisten te worden voldaan. De eerste is dat de (1) beperking bij 'wet' voorzien moet zijn, zoals een wet in materiële zin, beleidsregel of in de jurisprudentie gevormde regel. Deze wet of regel uit de jurisprudentie moet dan wel voor de burger toegankelijk zijn en verder zo nauwkeurig zijn dat de burger in staat is zijn concrete gedrag daarnaar te richten. Vervolgens moet de inmenging (2) noodzakelijk zijn voor de genoemde doeleinden en niet verder reiken dan strikt noodzakelijk is. Om noodzakelijk te zijn, dient de maatregel in elk geval relevant te zijn om het beoogde doel te bereiken. Vervolgens dient de maatregel (3) proportioneel te zijn, inhoudende dat er een redelijke verhouding tussen de aantasting van het recht op privacy enerzijds moet zijn en de legitieme doelstelling die nagestreefd wordt anderzijds. Tot slot dient de (4) inbreuk subsidiair te zijn, inhoudende dat de inbreuk op het recht op privacy zoveel mogelijk geminimaliseerd moet worden door alternatieve oplossingen te vergelijken.⁴²

§ 2.4.3 Europees Handvest van de Grondrechten van de Europese Unie

Naast het EVRM bestaat het Europese Handvest van de Grondrechten van de Europese Unie (hierna: Handvest) dat in 2009 in werking is getreden. In het Handvest zijn grondrechten en vrijheden van particulieren van de Europese Unie neergelegd, zoals het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens. Het Handvest dient er voor te zorgen dat de grondrechten binnen de Europese Unie in alle lidstaten gelijk zijn.⁴³

Het Handvest heeft dezelfde status als een verdrag.⁴⁴ Omdat dit verdrag in de toepasselijke artikelen 7 en 8 'eenieder' verbindt heeft dit artikel een directe werking.⁴⁵ De grondrechten die in het Handvest zijn opgenomen hebben een directe verticale werking, waardoor deze alleen voor particulieren ten opzichte van overheden van de verschillende

³⁸ Helm 2009, p. 41.

³⁹ EHRM 7 november 2002, 58341/00 (*Madsen/Denemarken*); EHRM 9 maart 2004, 46210/99 (*Wretlund/Zweden*).

⁴⁰ HR 14 september 2007, ECLI:NL:HR:2007:BA5802, r.o. 3.4.2.

⁴¹ Helm 2009, p. 41.

⁴² Hooghiemstra, p. 4; Helm 2009, p. 41; HR 13 juni 2011, ECLI:NL:PHR:2011:BQ8097, conclusie A-G mr. Verkade, punt 3.3;

⁴³ Hooghiemstra e.a. 2013, p. 3-5; Barents 2012, p. 22-23.

⁴⁴ art. 6 VEU.

⁴⁵ art. 7 en 8 Handvest jo. 93 jo. 94 Gw.

Europese lidstaten gelden en particulieren hierop bij de nationale rechter een beroep kunnen doen.⁴⁶ Of de bepalingen uit het Handvest ook een horizontale werking hebben is op dit moment nog onduidelijk. In toekomstige jurisprudentie zal dit verder moeten worden uitgekristalliseerd, waarbij de mogelijkheid bestaat dat de bepalingen uit het Handvest op den duur een horizontale werking zullen krijgen. Deze mogelijkheid is in recente jurisprudentie van het Hof van Justitie van de Europese Unie (hierna: HvJ EU) in het Laboubi-arrest aangegeven.⁴⁷ Daarom verwijs wordt in dit onderzoek toch naar de relevante artikelen uit het Handvest verwezen, ondanks het gegeven dat het Handvest op dit moment geen horizontale werking heeft. De toepasselijke artikelen 7 en 8 Handvest zien er als volgt uit:

'Artikel 7

Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en communicatie.'

'Artikel 8

1. Eenieder heeft recht op bescherming van persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd.'

§ 2.4.4 Nederlandse Grondwet

Naast de internationale en Europese grondrechten, die in de bovenstaande paragrafen aan bod zijn gekomen, is er een nationaal recht op privacy. Dit recht is in Nederland in de Grondwet (hierna: Gw) in artikel 10 Gw vastgelegd. Artikel 10 Gw ziet er als volgt uit:

'1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.

2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

*3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.'*⁴⁸

In lid 1 staat het recht op eerbiediging van de 'persoonlijke levenssfeer'. Dit is een zeer ruim begrip dat op talloze terreinen van toepassing kan zijn, waaronder het recht op privacy.⁴⁹ Daarnaast staat in dit lid dat dit recht op een 'ieder' van toepassing. Het recht op eerbiediging van de persoonlijke levenssfeer heeft door de formulering een directe werking.⁵⁰ Tevens is de regering van mening dat grondrechten ook waardevol zijn tussen particulieren onderling, waarbij de regering stelt dat per artikel bekeken dient te worden of er sprake is van een horizontale werking.⁵¹ Op grond van de mening die de regering heeft en het eerder genoemde arrest uit 1987 in subparagraaf 2.4.2, volgt dat dit artikel 10 lid 1 Gw tussen werkgever en werknemer van toepassing is en er dus sprake is van een directe horizontale werking.⁵²

⁴⁶ Hooghiemstra e.a. 2013, p. 3-5; art. 7 en 8 Handvest; Barents 2012, p. 119-120.

⁴⁷ Blokker e.a. 2014, p. 122, HvJ EU 15 januari 2014, C-176/12 (*Laboubi*).

⁴⁸ art. 10 Gw.

⁴⁹ Bunschoten 2010, aant. 2.

⁵⁰ art. 10 lid 1 Gw jo. 93 Gw.

⁵¹ *Kamerstukken II* 1975/76, 13 872, 3, p. 10 en 15-16.

⁵² Helm 2009, p. 32; HR 9 januari 1987, ECLI:NL:HR:1987:AG5500, r.o. 4.4.

Het recht op privacy, zoals in artikel 10 lid 1 Gw staat, kan 'bij of krachtens de wet' worden beperkt en is dus niet absoluut. Dit houdt in dat een beperking alleen door een wet die tot stand is gekomen door samenwerking tussen de regering en Staten-Generaal (wet in formele zin) of een wet in materiële zin, die krachtens een delegatiebepaling uit een wet in formele zin voortvloeit, kan worden beperkt.⁵³

Naast het bovengenoemde artikel 10 lid 1 Gw, geven de leden 2 en 3 van dit artikel de wetgever de opdracht om wetgeving op te stellen die regels bevatten ter bescherming van persoonsgegevens en kennisneming bij het vastleggen van persoonsgegevens. Een van de wetten die hier ondermeer uit voortvloeit, is de Wet bescherming persoonsgegevens, en ziet dus specifiek toe op de informationele privacy.⁵⁴

De Gw bevat ook meer specifiekere grondrechten waaronder het huisrecht en het brief-, telegraaf en telefoongeheim.⁵⁵ Omdat geen van deze artikelen van toepassing is op de communicatie via internet of het internetgebruik, worden deze in dit rapport buiten beschouwing gelaten. Desalniettemin heeft de Staatscommissie Grondwet in 2010 in een uitgebracht advies erop gewezen dat deze artikelen ook nieuwe technologieën (zoals e-mail en internet) moeten accepteren.⁵⁶ Het Kabinet Rutte II heeft hiertoe actie ondernomen.⁵⁷

§ 2.5 Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (hierna: Wbp) is een nationale wet en is sinds september 2001 van kracht, die de Wet persoonsregistratie heeft vervangen. De Wbp is in opdracht van artikel 10 leden 2 en 3 Gw en de Europese richtlijn⁵⁸, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens, tot stand gekomen.⁵⁹ Een Europese richtlijn is een bindende instructie vanuit de Europese Unie is en heeft een verticale werking. Het doel is om de onderlinge nationale wetgeving van de verschillende Europese lidstaten te bewerkstelligen en te harmoniseren.⁶⁰ Bij toepassing van de Wbp door nationale rechters, dient deze wet zoveel mogelijk in het licht van de bewoording en het doel van de richtlijn te worden uitgelegd.⁶¹

De Wbp wordt gezien als een kaderwet met een ruime toepassing, hierdoor is deze wet op diverse vormen van verwerking van persoonsgegevens en in verschillende sectoren van het maatschappelijk leven van toepassing. Ondanks deze reikwijdte blijkt uit het rapport 'Wat niet weet, wat niet deert', die door het Wetenschappelijk Onderzoek- en Documentatiecentrum is uitgebracht, dat de Wbp onder burgers onbekend is en daardoor niet erg leeft. Door deze onbekendheid, maar ook de mogelijkheid van geschillencommissies en het doen van een bemiddelingsverzoek bij het CBP, hebben ertoe geleid dat er weinig jurisprudentie over deze wet tot stand is gekomen, waardoor de Wbp in praktijk lastig is te hanteren.⁶² Ondanks deze beperkingen, zal de Wbp in deze paragraaf uitgebreid aan bod komen, om voor dit rapport een zo duidelijk en volledig mogelijk toetsingskader te schetsen.

Voordat de Wbp uiteen wordt gezet, heeft de Hoge Raad in 2011 bepaald dat de Wbp in overeenstemming met artikel 8 EVRM dient te worden uitgelegd, waarbij bovendien bij

⁵³ Helm 2009, p. 62.

⁵⁴ Bunschoten 2010, aant. 7; Zie paragraaf 2.3.

⁵⁵ art. 12 en 13 Gw.

⁵⁶ Rapport Staatscommissie Grondwet 2010, p. 85.

⁵⁷ Kamerstukken II 2014/15, 33989, 5.

⁵⁸ Richtlijn 95/46/EG (PbEG 1995 L 281/31).

⁵⁹ 'Wet bescherming persoonsgegevens', CBP, www.cpbweb.nl (zoek op *Wet bescherming persoonsgegevens*) (laatst geraadpleegd op 1 mei 2015); Vries & Rutgers 2001, p. 17.

⁶⁰ Kooijmans 2008, p. 286-288.

⁶¹ HvJ EG 13 november 1990, C-106/89 (*Marleasing*).

⁶² Winter e.a. 2008, p. 19 en 51.

elke gegevensverwerking moet zijn voldaan aan de beginselen van proportionaliteit en subsidiariteit.⁶³

§ 2.5.1 College Bescherming Persoonsgegevens

De Wbp heeft een eigen onafhankelijk college, genaamd het College Bescherming Persoonsgegevens (hierna: CBP), dat in Nederland toezicht houdt op de naleving van de Wbp. Naast het feit dat het CBP toezicht houdt op de naleving van de Wbp, is het ook een adviesorgaan van de Nederlandse regering en kan het bij niet-naleving van de wet bestuursdwang of bestuurlijke boetes opleggen.⁶⁴ In Europees verband is het CBP gezamenlijk met toezichthouders van de andere Europese lidstaten en de European Data Protection Supervisor⁶⁵, verenigd in de Artikel 29-werkgroep. Die werkgroep kan op verzoek van de Europese Commissie adviseren en uit eigen beweging aanbevelingen doen.⁶⁶

In deze paragraaf, maar ook in de rest van dit hoofdstuk, zullen adviezen en opinies van de Artikel 29-werkgroep en het herziene rapport 'Goed werken in netwerken' uit 2002 van het CBP, naast de wet- en regelgeving, literatuur en jurisprudentie worden toegepast. Het doel van dit CBP-rapport is een einde te maken aan het ontbreken van uniforme regels en te zeer uiteenlopende jurisprudentie op het gebied van (controle op) e-mail en internetgebruik.⁶⁷ Omdat dit rapport vuistregels voor de controle op e-mail- en internetgebruik bevat en het CBP de toezichthouder van de Wbp is, kunnen deze vuistregels als belangrijk en valide worden beschouwd. Hetzelfde geldt voor de adviezen en opinies van de Artikel 29-werkgroep.

§ 2.5.2 Reikwijdte

De Wbp is niet in alle gevallen van toepassing. Voor toepassing dient er te worden voldaan aan de reikwijdte die in artikel 2 lid 1 Wbp staat:

*'1. Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.'*⁶⁸

Ondanks deze brede reikwijdte bestaan een aantal uitzonderingen waarop de Wbp niet van toepassing is, zoals de verwerking van persoonsgegevens met persoonlijke of huishoudelijke doeleinden, voor inlichtingendiensten of de politietaak.⁶⁹ Aangezien geen van de uitzonderingen op dit onderzoek van toepassing is, worden deze verder in dit rapport buiten beschouwing gelaten.

Uit de bovenstaande reikwijdte komen een aantal elementen naar voren die in de volgende paragrafen nader worden gedefinieerd en uitgewerkt. Dit zijn:

- persoonsgegevens (subparagraaf 2.5.2.1);
- verwerking (subparagraaf 2.5.2.2);
- geheel of gedeeltelijk geautomatiseerde, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen (subparagraaf 2.5.2.3).

⁶³ HR 9 september 2011, ECLI:NL:HR:2011:BQ8097, r.o. 3.3.

⁶⁴ art. 51 jp. 52 Wbp; art. 65 en 66 Wbp.

⁶⁵ 'Artikel 29-werkgroep', CBP, cbpweb.nl (zoek op *EDPS*) (laatst geraadpleegd op 23 april 2015): Dit orgaan houdt toezicht op de verwerking van persoonsgegevens bij instellingen en organen van de EU.

⁶⁶ art. 41 Verordening (EG) 45/2001; Kranenborg & Verhey 2011, p. 31 en 52; 'Artikel 29-werkgroep', CBP, cbpweb.nl (zoek op *artikel 29-werkgroep*) (laatst geraadpleegd op 23 april 2015).

⁶⁷ Koevoets 2006, p. 194; Terstegge 2002, p. 2-3.

⁶⁸ art. 2 lid 1 Wbp.

⁶⁹ art. 2 lid 2 jo. 2 lid 3 Wbp.

§ 2.5.2.1 Persoonsgegevens

Het eerste element is dat er sprake dient te zijn van 'persoonsgegevens'. Dit begrip staat in artikel 1 sub a Wbp beschreven:

'a. persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'.⁷⁰

Uit deze omschrijving kunnen vervolgens weer vier elementen worden gehaald, die nader gedefinieerd worden. Het dient om 'elk gegeven' 'betreffende' een 'geïdentificeerde of identificeerbare' 'natuurlijke persoon' te gaan, voordat er sprake is van persoonsgegevens.

Elk gegeven

Het begrip 'gegeven' dient ruim te worden opgevat, dit is niet alleen tekst, maar bijvoorbeeld ook beeld en geluid. Het begrip 'elk' betekent dat er geen beperking is tot gegevens die iemands privéleven betreffen.⁷¹

Betreffende

Gegevens 'betreffende' een natuurlijke persoon kunnen duidelijk zijn vanuit hun aard, zoals een naam, adres, woonplaats, telefoonnummer⁷², camerabeelden of stemopname van een persoon, maar dit kan ook blijken uit de context waarin het gegeven wordt gebruikt. Omdat er voorheen veel onduidelijkheid bestond of er sprake is van een gegeven dat een persoon betreft, heeft de Artikel 29-werkgroep bepaalde criteria opgesteld. Volgens hen is er sprake van een gegeven dat een persoon betreft als er aan minimaal één van de volgende criteria is voldaan:⁷³

- inhoudelijk element Informatie over een persoon (bijvoorbeeld gegevens in een klantenbestand die betrekking hebben op een bepaald persoon);
- doelelement gegevens die (waarschijnlijk) gebruikt worden met het doel om iemand op een bepaalde manier te behandelen of diens status of gedrag te beoordelen of te beïnvloeden (bijvoorbeeld het bijhouden van prestatiegegevens en op grond daarvan de medewerker beoordelen);
- resultaatelment wanneer een gegeven waarschijnlijk invloed heeft op rechten en belangen van een persoon, zodanig dat die persoon daardoor anders wordt behandeld (bijvoorbeeld via GPS de locatie bepalen van een taxichauffeur).

(Direct of indirect) geïdentificeerd of identificeerbaar gegeven

Wanneer er sprake is van een gegeven, dan kan dit een 'geïdentificeerd of identificeerbaar' gegeven zijn. Hierbij gaat het erom of aan de hand van dit gegeven de identiteit van een persoon *redelijkerwijs*, zonder onevenredige inspanning (denk aan kosten, beoogde doel en de stand van de technologie ten tijde van de verwerking en de ontwikkelingen gedurende de periode dat de gegevens worden bewaard), kan worden vastgesteld. Het maakt hierbij geen verschil of deze identificatie ook daadwerkelijk plaats zal vinden.⁷⁴ Er is geen sprake van een persoonsgegeven, wanneer er doeltreffende (juridische en/of technische) maatregelen zijn getroffen als gevolg waarvan daadwerkelijke identificatie van natuurlijke personen redelijkerwijs wordt uitgesloten.⁷⁵ Een identificeerbaar gegeven kan vervolgens worden onderscheiden in een direct en

⁷⁰ art. 1 sub a Wbp.

⁷¹ Kranenborg & Verhey 2011, p. 60.

⁷² Rb. Dordrecht 31 augustus 2004, ECLI:NL:RBDOR:2004:AR5275.

⁷³ Rapport CBP Publicatie van persoonsgegevens op internet 2007, p. 9-10; Knol e.a. 2013, p. 725-726.

⁷⁴ Rapport CBP Publicatie van persoonsgegevens op internet 2007, p. 10; Knol e.a. 2013, p. 726-728.

⁷⁵ Kranenborg & Verhey 2011, p. 62.

indirect identificeerbaar gegeven. Een direct identificeerbaar gegeven is bijvoorbeeld de combinatie van de voor- en achternaam van een persoon. Een indirect identificeerbaar gegeven is een e-mailadres⁷⁶ of IP-adres. Ondanks dat in verschillende Europese lidstaten nog enige onduidelijkheid bestaat of een IP-adres een persoonsgegeven is, wordt hier in de Nederlandse jurisprudentie, het CBP en door de Artikel 29-werkroep wel vanuit gegaan.⁷⁷ Wellicht dat het HvJ EU, aan de hand van een prejudiciële vraag die door een Duitse rechter is gesteld, op korte termijn hierover meer duidelijkheid verschaft.⁷⁸

Natuurlijke persoon

Iedere levende natuurlijke persoon, zowel een Nederlandse als een buitenlandse onderdaan, kan aan de Wbp rechten ontleen. Gegevens die betrekking hebben op overledenen of rechtspersonen zijn geen persoonsgegevens, tenzij deze gegevens eveneens betrekking hebben op een nog levende natuurlijke persoon of in het geval het gaat om medische gegevens.⁷⁹

§ 2.5.2.2 Verwerking van persoonsgegevens

Het volgende element is de 'verwerking' van persoonsgegevens. Artikel 1 sub b Wbp definieert verwerking van persoonsgegevens als volgt:

*'b. verwerking: 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'.*⁸⁰

Door deze ruime wettelijke omschrijving, die een niet-limitatieve opsomming is, gaat het bij verwerking van persoonsgegevens om het gehele proces van verzamelen tot het moment van vernietigen van persoonsgegevens. Dit houdt in dat iedere handeling of ieder geheel van handelingen met betrekking tot een persoonsgegeven, dat al dan niet is uitgevoerd met behulp van geautomatiseerde werkwijzen, hieronder valt. Daarbij dient sprake te zijn van een zekere feitelijke macht over de persoonsgegevens. Deze feitelijke macht is aanwezig, wanneer het mogelijk is om enige invloed op de verwerking van deze gegevens uit te oefenen.⁸¹ Een telecomaandbieder die bijvoorbeeld gegevens louter doorvoert, zonder daarop enige invloed te kunnen uitoefenen, verwerkt geen persoonsgegevens.⁸²

§ 2.5.2.3 Geautomatiseerde of niet geautomatiseerde verwerking

Het laatste element is dat het dient te gaan om een 'geautomatiseerde verwerking' of 'niet geautomatiseerde verwerking'. Er is sprake van een geautomatiseerde verwerking als er gebruik wordt gemaakt van middelen en/of methoden van geautomatiseerde gegevensverwerking. Deze verwerking kan geheel of gedeeltelijk geautomatiseerd zijn, zoals het plaatsen van informatie op een internetpagina (uploaden is geautomatiseerd, toegankelijk maken van de website is handmatig).⁸³

Daarnaast valt ook de 'niet geautomatiseerde' verwerking (ook wel handmatige verwerking genoemd) van gegevens onder de reikwijdte van dit artikel, zolang deze

⁷⁶ Gerechtshof Amsterdam 18 juli 2002, ECLI:NL:GHAMS:2002:AE5514, r.o. 4.4.4.1.

⁷⁷ Knol e.a. 2013, p. 726-728; Terstegge 2002, p. 12.

⁷⁸ HvJ EU 17 december 2014, C-582/14 (*Breyer/Bondsrepubliek Duitsland*).

⁷⁹ 'Artikel 1 sub a Wbp', CBP, cbpweb.nl (zoek op *artikel 1 sub a persoonsgegevens*) (laatst geraadpleegd op 23 april 2015); Hooghiemstra 2013, p. 21; Kranenborg & Verhey 2011, p. 63-65.

⁸⁰ art. 1 sub b Wbp.

⁸¹ Knol e.a. 2013, p. 729; Vries & Rutgers 2001, p. 18.

⁸² Knol e.a. 2013, p. 729.

⁸³ Knol e.a. 2013, p. 737.

gegevens in een bestand zijn opgenomen of bestemd zijn om in een bestand te worden opgenomen. Wat een ‘bestand’ is geeft artikel 1 sub c Wbp aan:

*‘c. 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 verschillen personen’.*⁸⁴

Uit dit artikellid blijkt dat er sprake moet zijn van persoonsgegevens die betrekking hebben op verschillende personen én die in een gestructureerd geheel zijn opgenomen. Dit houdt in dat de gegevensverwerkingen of de verzameling op grond van meer dan één kenmerk een onderlinge samenhang moet vertonen. Onderlinge samenhang kan blijken uit een gemeenschappelijke bestemming of doel of wanneer de verzameling in de praktijk als een geheel dient te worden beschouwd. De tweede eis is dat het gestructureerde geheel van persoonsgegevens systematisch en gemakkelijk toegankelijk dient te zijn. Dit kan door een vooraf aangebrachte structuur of raadpleegmethodiek. De bestanden kunnen zowel op één locatie als op meerdere locaties verspreid staan, zolang deze verspreide bestanden als één geheel kunnen worden beschouwd, dus geen back-up bestanden.⁸⁵

§ 2.5.3 Verantwoordelijke en andere actoren

Naast de bovenstaande elementen dient er in Nederland een ‘verantwoordelijke’ aanwezig te zijn. De verantwoordelijke draagt zorg voor de naleving van de Wbp en de verplichtingen die in subparagraaf 2.5.4 en 2.5.5 aan bod komen.⁸⁶ Om te bepalen wie er als verantwoordelijke kan worden aangemerkt, moet naar de formeel-juridische zeggenschap worden gekeken. Dit kan een natuurlijke persoon of rechtspersoon zijn die, alleen of samen met anderen, het doel en de middelen (zoals een server) voor de verwerking van persoonsgegevens vaststelt.⁸⁷ Het gaat hierbij niet zozeer om degene die de feitelijke beslissingen neemt, maar om de natuurlijke persoon of rechtspersoon die formeel bevoegd is om deze beslissing(en) te nemen. Is het onduidelijk wie formeel-juridisch bevoegd is of zeggenschap heeft, dan moet er naar de in het maatschappelijk verkeer geldende maatstaven worden gekeken.⁸⁸ Vervolgens is bepalend bij de beoordeling of de onderneming in Nederland gevestigd is, of er in Nederland een vestiging met economische activiteit is, die niet een tijdelijke activiteit is, en betrokken is bij de verwerking van persoonsgegevens.⁸⁹ Wanneer de verantwoordelijke niet zelf in Nederland gevestigd is, maar in Nederland wel een vestiging heeft, zoals een bijkantoor, en daar persoonsgegevens in het kader van de activiteiten van die vestiging verwerkt, is de Wbp alsnog van toepassing.⁹⁰ Hierbij dient te worden opgemerkt dat er binnen een concern meerdere verantwoordelijken kunnen zijn.⁹¹

Naast een verantwoordelijke zijn er of kunnen er ook andere actoren betrokken zijn bij de verwerking van persoonsgegevens. Dit zijn een ‘bewerker’, ‘betrokkene’, ‘derde’ en/of ‘ontvanger’. De ‘bewerker’ is degene (persoon of instelling) die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan het rechtstreeks gezag van de verantwoordelijke te zijn onderworpen.⁹² Degene die binnen de organisatie van de verantwoordelijke of de bewerker werkzaam is en in dat verband met de verantwoordelijke of bewerker in hiërarchische relatie staat, is de ‘derde’.⁹³ De ‘betrokkene’ is degene over

⁸⁴ art. 1 sub c Wbp.

⁸⁵ Hooghiemstra 2013, p. 23; Knol e.a. 2013, p. 729-730; Kranenborg & Verhey 2011, p. 68.

⁸⁶ art. 15 Wbp.

⁸⁷ art. 1 sub d Wbp; Vries & Rutgers 2001, p. 19-20; *Kamerstukken II* 1997/98, 25 892, 3, p. 56.

⁸⁸ Sauerwein & Linnemann 2002, p. 17; Terstegge 2002, p. 22.

⁸⁹ ‘Artikel 4 lid 1 Wbp’, CBP, cbpweb.nl (zoek op *artikel 4 lid 1 verantwoordelijke*) (laatst geraadpleegd op 28 april 2015).

⁹⁰ Knol e.a. 2013, p. 741; Huydecoper 2006, p. 21; Hooghiemstra 2013 p. 23; Vries & Rutgers 2001, p. 20.

⁹¹ Huydecoper 2006, p. 22.

⁹² art. 1 sub e Wbp; Hooghiemstra 2013, p. 25; Kranenborg & Verhey 2011, p. 78.

⁹³ art. 1 sub g Wbp; Kranenborg & Verhey 2011, p. 80.

wie de gegevens informatie bevatten. Als de gegevens op meer dan één persoon betrekking hebben, dan is ieder van hen betrokkene.⁹⁴ Als 'ontvanger' wordt degene gezien aan wie de persoonsgegevens worden verstrekt. Dat kan zowel een persoon binnen de organisatie van de verantwoordelijke zijn als een persoon daarbuiten.⁹⁵

§ 2.5.4 Gewone en bijzondere persoonsgegevens

De Wbp maakt onderscheid tussen 'gewone' en 'bijzondere' persoonsgegevens, waarbij er een verschil bestaat in de rechtmatigheid van de verwerking daarvan. De bijzondere persoonsgegevens zijn gegevens die naar hun aard een bijzonder of gevoelig karakter hebben, zoals iemands gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke persoonsgegevens. Deze gegevens worden geacht de kern van de persoonlijke levenssfeer te raken en er kunnen bij de verwerking voor de betrokkene bijzondere risico's aan verbonden zitten. Om deze redenen is de verwerking daarvan in beginsel verboden. Dit verbod kan worden opgeheven, wanneer er op één van de in artikel 17 e.v. Wbp genoemde bepalingen een beroep kan worden gedaan.⁹⁶ De gewone persoonsgegevens zijn alle andere persoonsgegevens, die geen bijzondere persoonsgegevens zijn. Zowel de gewone als bijzondere persoonsgegevens, indien het verbod op de verwerking van deze bijzondere persoonsgegevens is opgeheven, mogen alleen worden verwerkt wanneer er aan de hierna genoemde vereisten wordt voldaan.

§ 2.5.5 Algemene beginselen verwerking persoonsgegevens

Bij de verwerking van persoonsgegevens dient de verantwoordelijke een aantal algemene wettelijke beginselen in acht te nemen, zodat de gegevensverwerking rechtmatig is en er sprake is van een rechtmatige beperking van het recht op privacy op grond van artikel 8 EVRM en 10 Gw. Deze wettelijke beginselen worden hierna uiteengezet.

§ 2.5.5.1 Rechtmatigheid algemeen

De algemene eis die de Wbp stelt is dat de verwerking van persoonsgegevens in overeenstemming moet zijn met de Wbp en andere wetgeving inzake de verwerking van persoonsgegevens. Met andere woorden: er moet sprake zijn van behoorlijke en zorgvuldige verwerking. Aan deze zorgvuldigheidsvereisten is voldaan indien de betrokkene(n) van de verwerking kennis kunnen nemen en indien zij volledig over de omstandigheden waaronder deze gegevens worden verkregen zijn ingelicht.⁹⁷ Wanneer de gegevens niet bij de betrokkene worden verkregen, geldt als uitgangspunt dat deze de betrokkene op het moment van vastlegging op de hoogte wordt gesteld. De verantwoordelijke deelt dan onder andere de betrokkene zijn identiteit en doeleinden van de verwerking mede.⁹⁸

§ 2.5.5.2 Doelbinding

De nadere eis voor de verwerking van persoonsgegevens is dat persoonsgegevens alleen voor een welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld (verkregen) mogen worden.⁹⁹ Dit houdt in dat er alvorens wordt overgegaan tot verzamelen van persoonsgegevens, er een precieze doelomschrijving aanwezig moet zijn. Deze omschrijving moet duidelijk en niet te ruim geformuleerd zijn. Vervolgens dient het doel of doeleinden, waarvoor deze gegevens verzameld worden rechtvaardig te zijn, inhoudende dat dit in alle stadia van de verwerking gerechtvaardigd moeten kunnen worden aan één van de in artikel 8 Wbp limitatief opgesomde rechtmatigheidsgronden.¹⁰⁰

⁹⁴ art. 1 sub f Wbp; Hooghiemstra 2013, p. 27.

⁹⁵ art. 1 sub h Wbp.

⁹⁶ art. 16 e.v. Wbp; Knol e.a. 2013, p. 765-766.

⁹⁷ art. 6 Wbp; 'Artikel 6 Wbp', CBP, cbpweb.nl (zoek op *artikel 6*) (laatst geraadpleegd op 29 april 2015).

⁹⁸ art. 33 jo. 34 Wbp; Kranenburg & Verhey 2011, p. 120.

⁹⁹ art. 7 jo. 1 sub o Wbp.

¹⁰⁰ 'Artikel 7 Wbp', CBP, cbpweb.nl (zoek op *artikel 7*) (laatst geraadpleegd op 29 april 2015); Knol e.a. 2013, p. 745.

§ 2.5.5.3 Rechtmatigheidsgronden

Voordat de rechtmatigheidsgronden uit artikel 8 Wbp worden behandeld, dient te worden opgemerkt dat elke gegevensverwerking, dus ook bij de aanwezigheid van een wettelijke rechtmatigheidsgrond, in overeenstemming met artikel 8 EVRM moet zijn. Daarvoor dient een belangenafweging aan de hand van de beginselen van proportionaliteit en subsidiariteit te worden gemaakt, die al eerder in subparagraaf 2.4.2 uiteen is gezet. Deze beginselen brengen met zich mee dat een inbreuk op de belangen van betrokkene niet onevenredig mogen zijn tot het met de verwerking te dienen doel, en dat dit doel in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze kan worden verwekelijkt. Wanneer er nadere gegevens worden verschaft, kan dit aanleiding geven tot een nieuwe en meer volledige afweging.¹⁰¹

De gronden voor een rechtmatige verwerking van persoonsgegevens uit artikel 8 sub a t/m f Wbp staan hieronder beschreven, waarvan alleen de gronden die voor dit rapport van belang kunnen zijn uitgebreid worden uitgewerkt.

1. Ondubbelzinnige toestemming van de betrokkene

De eerste grondslag om persoonsgegevens te mogen verwerken is vastgelegd in artikel 8 sub a Wbp. De verantwoordelijke mag de persoonsgegevens van de betrokkene verwerken, indien hij zijn ondubbelzinnige toestemming voor een specifieke verwerking heeft verleend. Dit houdt in dat er geen enkele twijfel over de gegeven toestemming van de betrokkene mag bestaan. Voor een ondubbelzinnige toestemming dient aan drie vereisten te worden voldaan.

- 1) De betrokkene dient zijn toestemming in vrijheid te geven, inhoudende dat hij een onafhankelijke positie bekleedt. Een werknemer kan in een afhankelijkheidspositie staan, daarom mag er niet te snel worden uitgegaan van een ondubbelzinnige en onafhankelijke toestemming.
- 2) De toestemming slechts op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerking toepassing is.
- 3) Als laatste dient de betrokkene voor een goede oordeelsvorming over de noodzakelijke inlichtingen te beschikken.¹⁰²

2. Noodzakelijk voor de uitvoering van een overeenkomst

De verwerking van persoonsgegevens is ook geoorloofd indien deze noodzakelijk is voor de uitvoering van een overeenkomst. Voorwaarde is dat de betrokkene zelf bij deze overeenkomst partij is.¹⁰³

3. Nakoming van een wettelijke verplichting

De verantwoordelijke is gerechtigd persoonsgegevens te verwerken indien dit noodzakelijk is om een op hem rustende wettelijke verplichting na te komen.¹⁰⁴

4. Vrijwaring van een vitaal belang van de betrokkene

Het moet hierbij gaan om een zaak van leven of dood, er moet dus sprake zijn van een dringende noodzaak. Bijvoorbeeld een situatie waarin medisch hulp dringend geboden is terwijl de betrokkene buiten bewustzijn is geraakt als gevolg van een ongeval.¹⁰⁵

5. Goede vervulling van een publiekrechtelijke taak

De verantwoordelijke is gerechtigd persoonsgegevens te verwerken voor zover deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak.¹⁰⁶

¹⁰¹ HR 9 september 2011, ECLI:NL:HR:2011:BQ8097, r.o. 3.3.

¹⁰² art. 8 sub a Wbp; Hooghiemstra 2013, p. 27; Knol e.a. 2013, p. 747.

¹⁰³ art. 8 sub b Wbp; Knol e.a. 2013, p. 749.

¹⁰⁴ art. 8 sub c Wbp; Knol e.a. 2013, p. 749.

¹⁰⁵ art. 8 sub d Wbp; Knol e.a. 2013, p. 750.

¹⁰⁶ art. 8 sub e Wbp. Knol e.a. 2013, p. 751.

6. Behartiging van een gerechtvaardigd belang van de verantwoordelijke of van een derde
Dit is de laatste rechtmatigheidsgrond dat volgens Artikel 29-werkgroep niet als “vangnet” of “laatste kans” mag worden gezien.¹⁰⁷ Hier dient de verwerking van persoonsgegevens noodzakelijk te zijn voor het gerechtvaardigd belang van de verantwoordelijke of derde aan wie de persoonsgegevens worden verstrekt, tenzij het belang van de grondrechten en vrijheden van de betrokkene prevaleert.¹⁰⁸

Gerechtvaardigd belang

Wanneer er sprake is van een gerechtvaardigd belang is lastig vast te stellen, maar wordt in ieder geval aanwezig geacht als de betreffende verwerking noodzakelijk is om de reguliere bedrijfsactiviteiten te kunnen verrichten. Tevens ook ten aanzien van gegevensverwerking die geen onderdeel uitmaken van de reguliere bedrijfsactiviteiten van de verantwoordelijke, maar die wel in wezenlijke zin ondersteunen, kan in de regel worden aangenomen dat de verantwoordelijke een gerechtvaardigd belang heeft. Voorbeelden zijn fraudebestrijding en intern marktonderzoek.¹⁰⁹ Ook de controle op gedragsregels en bij een gerechtvaardigde verdenking van overtreding van de binnen de organisatie geldende regels door een werknemer, zoals een controle op overmatig internetgebruik voor privédoeleinden, is een gerechtvaardigd belang.¹¹⁰ Omdat het vaststellen van een gerechtvaardigd belang in de praktijk erg lastig is en dit artikel vanuit de Richtlijn 95/46/EG een rechtstreekse werking heeft, wordt er naar een advies van de Artikel 29-werkgroep gekeken.¹¹¹ In dit advies heeft de werkgroep “handvatten” aangeboden om het gerechtvaardigd belang te toetsen:

- het belang moet in overeenstemming met het Europese en nationale recht zijn (ook wel rechtmatig);
- het belang moet voldoende zeker en specifiek omschreven zijn, zodat de afweging van het belang van de verantwoordelijke of derde kan worden afgewogen tegen het belang van de betrokkene met betrekking tot de fundamentele rechten; en
- het moet gaan om een huidig en echt belang, dat niet speculatief is.¹¹²

Noodzakelijk

Naast het gerechtvaardigde belang, dient de gegevensverwerking noodzakelijk te zijn voor de verantwoordelijke of derde. Daarvoor dient een afweging plaats te vinden, tussen het belang van de verantwoordelijke of derde en die van de betrokkene. Waarbij de belangen van de betrokkene een zelfstandig gewicht krijgen tegenover het belang van de verantwoordelijke.¹¹³ Tevens dient deze afweging aan de hand van de rechtsverhouding tussen partijen te worden ingekleurd. Inhoudende dat er in een geval van een ongelijkwaardige verhouding daarmee rekening moet worden gehouden, waardoor degene met de sterkste positie een minder ruime beoordelingsvrijheid toekomt, dan dit bij een gelijkwaardige verhouding zou zijn.¹¹⁴ Om aan de noodzakelijkeis te voldoen, dienen de onderstaande vragen bevredigend te worden beantwoord, waarmee tevens wordt voldaan aan een impliciete motiveringsplicht van de verantwoordelijke en voor een eventuele toetsing bij de rechter:¹¹⁵

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

¹⁰⁷ Opinie 06/2014 Artikel 29-werkgroep, p. 49.

¹⁰⁸ art. 8 sub f Wbp; Knol e.a. 2013, p. 751-752.

¹⁰⁹ Kamerstukken II 1997/98, 25 892, 3, p. 86-87; Hooghiemstra 2013, p. 51.

¹¹⁰ Vries & Rutgers 2001, p. 78; Terstegge 2002, p. 22-23; Berkvens e.a. 2007, p. 198.

¹¹¹ Knol e.a. 2013, p. 752.

¹¹² Opinie 06/2014 Artikel 29-werkgroep, p. 49.

¹¹³ Hooghiemstra 2013, p. 51; Knol e.a. 2013, p. 752.

¹¹⁴ Kranenborg & Verhey 2011, p. 90.

¹¹⁵ Kamerstukken II 1997/98, 25 892, 3, p. 86; Vries & Rutgers 2001, p. 26-27.

- 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?
- Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg - zonder verwerking - worden bereikt?
- Is de verwerking in de mate die is beoogd evenredig aan het nagestreefde doel?¹¹⁶

Om als verantwoordelijke nog meer verzekerd te zijn dat er voldaan is aan de noodzakelijke eisen, is het mogelijk om een extra toetsing aan de hand van de regels uit een opinie van de Artikel 29-werkgroep uit te voeren. Deze opinie is deels herhaling van hetgeen hierboven al genoemd is, dit wordt hier niet opnieuw benoemd. Er dient een eindbalans te worden opgemaakt, waarin naar extra of aanvullende waarborgen wordt gezocht en die vervolgens ook worden geïmplementeerd. Door deze waarborgen te implementeren kan 'het voordeel', bij twijfel over de voldoening aan de noodzakelijke eisen, kantelen in de richting van de verantwoordelijke en worden de betrokkenen tevens ook (extra) beschermd. Er dient te worden aangetoond dat aan de bovenstaande punten is voldaan. En dat de betrokkenen zijn geïnformeerd over de redenen en het feit dat de verantwoordelijke het recht op de controle van internetgebruik van een werknemer heeft. De bovenstaande uitgewerkte punten dient de verantwoordelijke altijd te hebben, zodat men zich bij een eventuele controle van het CBP kan verantwoorden. Wanneer een betrokkene zich verzet, dienen de rechten van betrokkenen opnieuw te worden bekeken en afgewogen.¹¹⁷

§ 2.5.5.4 Verenigbaar gebruik

Wanneer de persoonsgegevens op een rechtmatige grond worden verwerkt, mogen deze alleen voor doeleinden gebruikt worden waarvoor deze zijn verzameld. Verdere verwerking is geoorloofd, mits dit verenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verkregen. Dit dient aan de hand van de niet-limitatieve opsomming uit artikel 9 lid 2 Wbp verder te worden bezien, waarbij geen van de opgesomde factoren van doorslaggevende betekenis is. De uitzondering die in de leden 3 of 4 van dit artikel staan, zijn voor dit onderzoek niet van toepassing en wordt om die reden buiten beschouwing gelaten.¹¹⁸

§ 2.5.5.5 Kwaliteit en bewaartermijn

De verantwoordelijke dient zorg voor te dragen dat de gegevens slechts mogen worden verwerkt als deze toereikend, ter zake dienend voor het doeleind of doeleinden zijn en niet bovenmatig zijn.¹¹⁹ Daarnaast dienen deze gegevens met de nodige (in redelijkheid te stellen) maatregelen juist en nauwkeurig te zijn, waardoor voldoende (niet te veel en niet te weinig) gegevens worden verzameld om, zoals eerder gezegd, toereikend voor het doeleinde te zijn.¹²⁰ Dit ter voorkoming van beslissingen die gebaseerd zijn op onvolledige informatie. Kortom: niet te veel, maar ook niet te weinig persoonsgegevens verwerken. Daarnaast mogen de gegevens niet langer dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of worden verwerkt, in een vorm die het mogelijk maakt de betrokkene te identificeren worden bewaard.¹²¹ De maximale bewaartermijn voor persoonsgegevens van het internet is maximaal zes maanden, dan

¹¹⁶ *Kamerstukken II 1997/98*, 25 892, 3, p. 86.

¹¹⁷ *Opinie 06/2014 Artikel 29-werkgroep*, p. 55-56.

¹¹⁸ art. 9 lid 1 jo lid 2 Wbp; Knol 2013 e.a., p. 756-758; Vries & Rutgers 2001, p. 28.

¹¹⁹ art. 11 lid 1 Wbp; 'Artikel 11 lid 1 Wbp', CBP, cbpweb.nl (zoek op *artikel 11 lid 1*) (laatst geraadpleegd op 1 mei 2015).

¹²⁰ art. 11 lid 2 Wbp; 'Artikel 11 lid 2 Wbp', CBP, cbpweb.nl (zoek op *artikel 11 lid 2*) (laatst geraadpleegd op 1 mei 2015); Vries & Rutgers 2001, p. 29-30.

¹²¹ art. 10 lid 1 Wbp.

wel twee jaren nadat het dienstverband of de werkzaamheden van betrokkene ten behoeve van de verantwoordelijke is beëindigd.¹²²

§ 2.5.5.6 Beveiliging en geheimhouding

De verantwoordelijke dient passende (denk aan kosten van de maatregel(en) en de stand van de techniek) technische en organisatorische (beveiligings)maatregelen te nemen, om verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens te voorkomen. De hoogte of zwaarte van de beveiliging hangt af van de aard en de context waarin de gegevens worden gebruikt, denk aan gevoelige gegevens.¹²³ Hierbij vormt software, zoals versleutelingstechnologieën, een belangrijk instrument.¹²⁴ Degene die deze gegevens verwerkt of toegang hebben tot deze gegevens hebben een geheimhoudingsplicht.¹²⁵ Verder heeft de verantwoordelijke de taak om zorg te dragen voor de naleving van een groot deel van de bovengenoemde verplichtingen. Wanneer de verantwoordelijke niet aan deze verplichtingen voldoet is hij aansprakelijk.¹²⁶

§ 2.5.5.7 Meldplicht en voorafgaand onderzoek

Het geheel of gedeeltelijk geautomatiseerd verwerken van persoonsgegevens, die voor verwezenlijking van een doeleinde of verscheidene samenhangende doeleinden bestemd is, dient door de verantwoordelijke vóór de verwerking bij het CBP of een functionaris binnen de (eigen) organisatie te worden gemeld.¹²⁷ Dit geldt op grond van het transparantiebeginsel.¹²⁸ De melding dient aan de opgesomde vereisten in artikel 28 Wbp te voldoen. Ondanks dat de verantwoordelijke in veel gevallen verplicht is om daarvan bij het CBP melding te maken, is dit in bepaalde gevallen op grond van het Vrijstellingsbesluit Wbp niet nodig.¹²⁹ Zo geldt deze meldingsplicht in beginsel niet wanneer de verantwoordelijke het internetgebruik van zijn werknemers controleert en aan de in het Vrijstellingsbesluit Wbp genoemde vereisten voldoet, waaronder de verkregen instemming van de ondernemingsraad (hierna: OR).¹³⁰ In bijzondere gevallen, zoals bij een heimelijke controle die in subparagraaf 2.6.1 aan bod komt, dient het CBP een voorafgaand onderzoek in te stellen voordat er kan worden overgegaan tot heimelijke controle van een werknemer.¹³¹

§ 2.5.5.8 Rechten van betrokkenen

De Wbp kent de betrokkenen een aantal rechten toe, zoals recht op kennisneming¹³² en het recht van verzet¹³³. Deze rechten worden in dit rapport niet verder behandeld, omdat deze niet tot het doel van dit rapport behoren.

§ 2.6 Arbeidsrechtelijk kader

De meeste werknemers komen wanneer ze in dienst treden met de werkgever een individuele arbeidsovereenkomst overeen. Deze individuele arbeidsovereenkomst is in artikel 7:610 Burgerlijk Wetboek (hierna: BW) geregeld. Op grond daarvan is het arbeidsrecht in Boek 7 Titel 10 Burgerlijk Wetboek van toepassing, waardoor de bepalingen uit deze titel op de werkgever en werknemer van toepassing zijn.¹³⁴

¹²² art. 32 lid 6 Vrijstellingsbesluit Wbp.

¹²³ art. 13 Wbp; Knol e.a. 2013, p. 762.

¹²⁴ Vries & Rutgers 2001, p. 30.

¹²⁵ art. 12 Wbp; Knol e.a. 2013, p. 760-761.

¹²⁶ art. 15 jo. 65 Wbp.

¹²⁷ art. 27 lid 1 jo. lid 3 jo. 1 sub I jo. 62 Wbp.

¹²⁸ 'Artikel 27 lid 1 Wbp', CBP, cbpweb.nl (zoek op *artikel 27 lid 1*) (laatst geraadpleegd op 1 mei 2015).

¹²⁹ art. 29 Wbp.

¹³⁰ Terstegge 2002, p. 23-24; art. 29 lid 1 jo. 27 Wbp jo. art. 32 lid 1 jo. 32 lid 3 sub c Vrijstellingsbesluit Wbp; art. 32 lid 4 en 5 en 6 Vrijstellingsbesluit Wbp; *Stb.* 2001, 250, p. 69.

¹³¹ art. 31 jo. 32 Wbp.

¹³² art. 35 Wbp.

¹³³ art. 40 en 41 Wbp.

¹³⁴ art. 7:610 lid 2 BW.

In de individuele arbeidsovereenkomsten kunnen regels zijn opgenomen, waaraan de werknemer zich dient te houden. Doordat de werknemer deze overeenkomst heeft ondertekend, heeft hij met deze regels expliciet ingestemd en is hij gehouden deze regels na te leven.¹³⁵

Krachtens de bepalingen uit het arbeidsrecht is de werkgever op grond van de instructiebevoegdheid uit artikel 7:660 BW bevoegd tot het geven van voorschriften (hierna: regels, dit zijn eenzijdige bindende aanwijzingen) voor het verrichten van arbeid en het nemen van maatregelen ter bevordering van de goede orde in de onderneming. De werknemer is op grond van deze instructiebevoegdheid verplicht zich te houden aan de regels die de werkgever oplegt.¹³⁶ Bij het opleggen van deze regels dient de werkgever rekening te houden met het goed werkgeverschap in artikel 7:611 BW. Dit artikel houdt in dat de werkgever zich als een 'goed werkgever' dient te gedragen. Op zijn beurt dient de werknemer zich ook als een 'goed werknemer' te gedragen. Samen worden dit ook het 'goed werkgever- en werknemerschap' genoemd, dat een arbeidsrechtelijke open norm is en door de redelijkheid en billijkheid uit artikel 6:2 en 6:248 BW wordt ingevuld.¹³⁷ De werkgever dient niet alleen rekening te houden met het goed werkgeverschap, maar ook met andere wettelijke bepalingen en hetgeen overeengekomen is in de individuele of collectieve arbeidsovereenkomst (hierna: CAO).¹³⁸ De regels omtrent hetgeen dat is toegestaan en verboden is, dienen helder naar de werknemer te zijn gecommuniceerd en periodiek te worden geëvalueerd. Wanneer het regels zijn die online gelden, dan dienen deze in overeenstemming te zijn met hetgeen dat offline geldt.¹³⁹

§ 2.6.1 Controlebevoegdheid

Een werkgever kan zijn bevoegdheid tot het controleren van werknemers baseren op de wettelijke instructiebevoegdheid uit artikel 7:660 BW en het goed werknemerschap, in combinatie met de bijzondere contractuele vertrouwensrelatie tussen de werkgever en werknemer (zie paragraaf 2.6). Van deze bevoegdheid kan alleen gebruik worden gemaakt, wanneer de werkgever een vermoeden heeft dat een werknemer zich niet aan de uit deze vertrouwensrelatie voortvloeiende verplichtingen houdt.¹⁴⁰ Dit geldt ook voor internetgebruik.¹⁴¹

Open onderzoek of heimelijke controle

Binnen de arbeidsverhouding wordt er onderscheid gemaakt in twee soorten controles. Dit zijn het 'open onderzoek' en de 'heimelijke controle', dat ook op internetgebruik van werknemers kan plaatsvinden. Beide vormen van controle dienen aan de Wbp-vereisten genoemd in paragraaf 2.5 te voldoen, waarbij extra vereisten kunnen gelden die hieronder worden benoemd.

Het open onderzoek houdt in dat de werknemer die wordt gecontroleerd voorafgaand aan het onderzoek daarvan op de hoogte is gesteld (kenbaarheidsvereiste). Hier kan aan worden voldaan door ondubbelzinnige toestemming voorafgaand aan de controle van de werknemer te hebben verkregen (artikel 8 sub a Wbp) of een reglement te hebben met daarin opgenomen de controlemogelijkheden en regels voor werknemers wat verboden en toegestaan is (voorkeur heeft dat de werknemer hiermee expliciet heeft ingestemd).¹⁴² De tweede onderzoeksmogelijkheid is de heimelijke controle, waarbij de werknemer niet voorafgaand aan de controle op de hoogte is gesteld. Hierbij ontbreekt dus het kenbaarheidsvereiste. Voor deze controle gelden buiten de regels die voor het open

¹³⁵ Verhulp & Zondag 2008, p. 8-9.

¹³⁶ Verhulp & Zondag 2008, p. 9.

¹³⁷ HR 8 april 1994, ECLI:NL:HR:1994:ZC1322, m.nt. P.A. Stein, r.o. 10; Koevoets 2006, p. 206.

¹³⁸ Koevoets 2006, p. 206.

¹³⁹ Terstegge 2002, p. 31 en 34.

¹⁴⁰ Koevoets 2006, p. 11-12.

¹⁴¹ Terstegge 2002, p. 34.

¹⁴² Dancet e.a. 2013, p. 70-71; 'Controle van personeel', CBP, cbpweb.nl (zoek op *heimelijke controle*) (laatst geraadpleegd op 19 mei 2015); Vries & Rutgers 2001, p. 77.

onderzoek gelden, nog een aantal extra vereisten. Zo mag een werkgever de heimelijke controle enkel inzetten als ultimum remedium. Dit kan uit het goed werknemer- en werkgeverschap en de Arbeidsomstandighedenregeling dat toeziet op het gebruik van controlemechanismen worden begrepen.¹⁴³ Andere middelen dienen dus uitgeput te zijn. Toch is het uitvoeren van een heimelijke controle onder bijzondere omstandigheden toegestaan. Bijvoorbeeld in het kader van fraudebestrijding. Daarvoor gelden een aantal extra vereisten. In eerste instantie dient de mogelijkheid van heimelijke controle binnen de organisatie bekend te zijn. Om een gerechtvaardigd belang bij de controle te hebben (artikel 8 sub f Wbp) dient er voor de werkgever een zwaarwegend belang in het geding te zijn, waarbij tevens sprake is van een gerichte redelijke verdenking ten aanzien van één of meerdere werknemers die handelingen verrichten die strafbaar of verboden zijn.¹⁴⁴

Voor beide controles gelden de onderstaande regels van het CBP:

- Het aangewezen tijdstip om de controlemogelijkheid op internetgebruik te melden is bij het opstarten van het (computer)systeem of het programma. Daardoor wordt gegarandeerd dat de werknemers zich bewust zijn van de geldende regels.¹⁴⁵
- Onafgebroken controleren van werknemers is niet toegestaan, dit is zowel schadelijk voor de gezondheid en het welzijn van werknemers, als in strijd met het goed werkgeverschap.¹⁴⁶
- Controle moet zijn voorzien van maatwerk, inhoudende dat er eerst een selectie van verdachte en niet-verdachte werknemers of computers dient te worden gemaakt. Hieruit worden de verdachte werknemers of computers gescreend op het onderschepte internetverkeer, waarbij de controle in beginsel moet zijn beperkt tot de verkeersgegevens.¹⁴⁷ Deze gegevens geven inzicht in bijvoorbeeld de datum, de tijd en het internetgedrag.¹⁴⁸ Hier dient bij hetgeen de minste of kleinste inbreuk op het recht op privacy maakt te worden begonnen.
- Wanneer geconstateerd wordt dat een werknemer de regels overtreedt dient die werknemer zo spoedig mogelijk op dat gedrag te worden aangesproken. Een zekere tijd voor dossieropbouw is toegestaan, indien de omstandigheden daartoe aanleiding geven.¹⁴⁹

Controle bij thuiswerken

Binnen verschillende ondernemingen is het voor werknemers vaak mogelijk om vanuit huis op het bedrijfsnetwerk in te loggen. Hierdoor kan er een extra privacyprobleem worden gevormd. Wanneer werknemers uitsluitend ten behoeve van het werk inloggen, vormt het vanuit huis inloggen geen beletsel. De werknemer die inlogt maakt immers logisch gezien, net zoals wanneer vanuit kantoor wordt inlogt, deel uit van het bedrijfsnetwerk. Daardoor bevindt deze werknemer zich dan ook in een situatie waarin de arbeidsgezagsverhouding geldt. Maar als de werknemer vanuit huis op het bedrijfsnetwerk inlogt en hier dan ook voor privédoeleinden gebruik van mag maken of in privétijd op het internet mag surfen, dan is voor zijn privéhandelingen geen grond voor registratie. Dit laatste geldt zeker wanneer gezinsleden ook van deze middelen gebruik mogen maken.¹⁵⁰ De vraag wanneer er sprake is van privé- en werktijd valt buiten de reikwijdte van dit onderzoek en zal daarom niet verder worden besproken.

¹⁴³ Dancet e.a. 2013, p. 70-71; art. 7:611 BW en art. 5.3 sub c Arbeidsomstandighedenregeling; 'Controle van personeel', CBP, cbpweb.nl (zoek op *heimelijke controle*) (laatst geraadpleegd op 19 mei 2015).

¹⁴⁴ Knol e.a. 2013, p. 755.

¹⁴⁵ Terstegge 2002, p. 31-32.

¹⁴⁶ Terstegge 2002, p. 32.

¹⁴⁷ Terstegge 2002, p. 38.

¹⁴⁸ Terstegge 2002, p. 22.

¹⁴⁹ Terstegge 2002, p. 33.

¹⁵⁰ Terstegge 2002, p. 16.

§ 2.6.2 Overmatig internetgebruik voor privédoeleinden

Het internet kan zowel voor zakelijke doeleinden als voor privédoeleinden worden gebruikt. In de meeste gevallen zal de werkgever niet spreken van “overmatig internetgebruik voor zakelijke doeleinden”, omdat de werknemer zijn taak uitvoert en het dus noodzakelijk acht om gebruik te maken van het internet. Daarentegen zal de werkgever het “overmatige internetgebruik voor privédoeleinden” niet tolereren. Er is geen wettelijke definitie van het begrip ‘privédoeleinden’. De Van Dale beschrijft dat het woord ‘privé’, als ‘persoonlijk’.¹⁵¹ Uit deze omschrijving kan dus worden opgemaakt dat het doel van het internetgebruik voor privédoeleinden, dus een persoonlijk doel voor de werknemer moet hebben.

Het gebruik van het internet is tijdens werktijd voor privédoeleinden binnen zekere grenzen toegestaan, zo blijkt uit uitspraken van het EHRM¹⁵², de nationale rechter¹⁵³ en het CBP¹⁵⁴ (zie ook paragraaf 2.5). Wanneer er sprake is van overmatig internetgebruik voor privédoeleinden staat nergens in de wet beschreven. Daarvoor dient bij de arbeidsrechtelijke jurisprudentie te worden aangesloten. Hieruit vloeit voort er sprake is van overmatig internetgebruik voor privédoeleinden, wanneer een werknemer aan het internetgebruik voor privédoeleinden buitenproportioneel veel tijd besteed of dit gebruik ernstig ten koste gaat van de werkzaamheden.¹⁵⁵ Tevens mag dit gebruik ook in geen geval storend zijn voor de werkzaamheden.¹⁵⁶ In de jurisprudentie wordt twintig uur per week, ook wel de helft van de werkweek (arbeidsduur), als ‘excessief’ beschouwd.¹⁵⁷ Omdat er verder geen jurisprudentie is, dat dit onderwerp beschrijft, blijft het lastig te bepalen wanneer er precies sprake is van overmatig internetgebruik. Om die reden zullen de bovenstaande uitspraken als handvatten dienen om het internetgebruik van een werknemer te toetsen.

Wanneer er een gang naar de rechter wordt gemaakt, dient het overmatige internetgebruik door de werkgever aan de hand van een lijst met de door werknemer bezochte internetwebsites en het daadwerkelijke data-verkeer (dat de intensiteit van het internetgebruik weergeeft) te worden overlegd. Door niet alleen de bezochte internetwebsites te overleggen, maar ook het data-verkeer, wordt voorkomen dat deze werknemer foutief wordt beoordeeld op het gebruik of bezoeken van internetwebsites.¹⁵⁸

§ 2.6.3 Wet op de Ondernemingsraden

Krachtens artikel 2 Wet op de ondernemingsraad (hierna: WOR) dient elke onderneming met 50 of meer werknemers een OR in te stellen. Bij twee of meer ondernemingsraden kan er ook een centrale ondernemingsraad (hierna: COR) worden ingesteld.¹⁵⁹ De OR heeft een aantal bevoegdheden, waaronder het instemmingsrecht. Dit recht heeft een onderneming bij verschillende besluiten nodig. Het instemmingsrecht heeft de (C)OR onder andere bij een voorgenomen besluit tot vaststelling, wijziging of intrekking van:

- een regeling omtrent het verwerken van alsmede de bescherming van persoonsgegevens van de in de onderneming werkzame personen;¹⁶⁰
- een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen.¹⁶¹

¹⁵¹ ‘Privé’, Van Dale, www.vandale.nl (zoek op *privé*) (laatst geraadpleegd op 25 april 2015).

¹⁵² EHRM 3 april 2007, ECLI:NL:XX:2007:BA6786, NJ 2007,617 (*Copland/Verenigd Koninkrijk*).

¹⁵³ Rb. Midden-Nederland (ktr.) 30 april 2014, ECLI:NL:RBMNE:2014:1751, r.o. 4.10.

¹⁵⁴ Terstegge 2002, p. 32.

¹⁵⁵ Rb. Midden-Nederland (ktr.) 30 april 2014, ECLI:NL:RBMNE:2014:1751, r.o. 4.10.

¹⁵⁶ CRvB 28 augustus 2014, ECLI:NL:CRVB:2014:2974, r.o. 3.2.

¹⁵⁷ Rb. Oost-Nederland (zittingplaats Almelo) 21 maart 2013, ECLI:NL:RBONE:2013:BZ5412 r.o. 3.11 en CRvB 28 augustus 2014, ECLI:NL:CRVB:2014:2974, r.o. 3.2.

¹⁵⁸ Rb. Maastricht (ktr.) 1 oktober 2009, ECLI:NL:RBMAA:2009:BJ9222.

¹⁵⁹ art. 33 lid 1 WOR.

¹⁶⁰ art. 27 lid 1 sub k WOR.

Onder het instemmingsrecht valt volgens het CBP ook het open onderzoek en heimelijke controle op internetgebruik.¹⁶² Dit betekent dat voorafgaand aan een open onderzoek of heimelijke controle instemming van de (C)OR noodzakelijk is.

§ 2.6.4 Sanctiebevoegdheid

De werkgever kan op grond van drie gronden bevoegd zijn tot het sanctioneren van zijn werknemers.

De eerste mogelijkheid is dat in de individuele arbeidsovereenkomst of de CAO die op deze arbeidsovereenkomst van toepassing is, sancties zijn opgenomen die bij overtreding van de regels kunnen worden opgelegd. Door ondertekening van de individuele arbeidsovereenkomst heeft een werknemer expliciet met deze regels ingestemd en kunnen de sancties worden opgelegd.¹⁶³

Een tweede mogelijkheid is dat de werkgever geen regels in de individuele arbeidsovereenkomst of CAO heeft opgenomen. Dan kan de werkgever zich beroepen op het feit dat er een individuele arbeidsovereenkomst gesloten is. Op grond van deze arbeidsovereenkomst is een werknemer volgens artikel 7:610 lid 1 BW 'in dienst van' de werkgever en om die reden onderworpen aan het instructierecht van de werkgever.¹⁶⁴

De laatste mogelijkheid, die in paragraaf 2.6 al aan de orde kwam, is de wettelijke instructiebevoegdheid op grond van artikel 7:660 BW. Op grond van dit recht is de werkgever bevoegd tot het nemen van maatregelen ter bevordering van de goede orde in de onderneming.¹⁶⁵

Wanneer een werknemer de opgestelde regels overtreedt of in strijd handelt met het goed werknemerschap, is de werkgever bevoegd disciplinaire maatregelen of sanctie op te leggen, waarmee het terrein van het arbeidstuchtrecht wordt betreden.¹⁶⁶ Voor dit recht ontbreken wettelijke regels, met uitzondering van de grondslag voor het opleggen van een boete. Omdat er geen wettelijke regels omtrent het arbeidstuchtrecht zijn, wordt dit onderwerp uiteengezet aan de hand van jurisprudentie en literatuur.¹⁶⁷

§ 2.6.4.1 Sanctie

De literatuur maakt geen onderscheid in 'disciplinaire maatregelen' en 'sancties'. Om deze reden wordt hier aangesloten bij het begrip sanctie. Het begrip 'sanctie' is geen wettelijke term. De Van Dale beschrijft het begrip sanctie onder andere als 'bekrachtiging' of 'straf waarmee wordt gedreigd'.¹⁶⁸ In de literatuur wordt dit begrip als volgt omschreven:

- 1) Het dient te gaan om een reactie op de schending van een (rechts)norm of -regel, althans verplichting, dan wel onrechtmatig of onwettig gedrag.
- 2) Ten tweede wordt degene die de rechtsnorm of -regel heeft geschonden door de reactie in zijn belangen getroffen, of heeft de reactie in ieder geval nadelige gevolgen voor de werknemer.¹⁶⁹

De werknemer moet dus in eerste instantie een (rechts)norm of (rechts)regel schenden of zich onwettig gedragen, waarop een reactie plaatsvindt die de werknemer in zijn belangen treft of nadelige gevolgen heeft. Wanneer hiervan sprake is, is er sprake van een sanctie.

¹⁶¹ art. 27 lid 1 sub I WOR.

¹⁶² Terstegge 2002, p. 21; 'Controle van personeel', CBP, cbpweb.nl (zoek op *heimelijke controle*) (laatst geraadpleegd op 19 mei 2015).

¹⁶³ Verhulp & Zondag 2008, p. 8-9.

¹⁶⁴ Verhulp & Zondag 2008, p. 9.

¹⁶⁵ Verhulp & Zondag 2008, p. 9.

¹⁶⁶ Verhulp & Zondag 2008, p. 7.

¹⁶⁷ Verhulp & Zondag 2008, p. 50.

¹⁶⁸ 'Sanctie', Van Dale, www.vandale.nl (zoek op *sanctie*) (laatst geraadpleegd op 24 april 2015).

¹⁶⁹ Koevoets 2006, p. 104.

§ 2.6.4.2 Soorten sancties

Specifieke wettelijke sancties, die bij overtreding van de regels omtrent internetgebruik kunnen worden opgelegd, bestaan niet. Om die reden wordt aangesloten bij de mogelijkheden die in de jurisprudentie en literatuur doorgaans als arbeidsrechtelijke sanctie worden beschouwd. Dit zijn:

- de officiële waarschuwing;
- de officiële berisping;¹⁷⁰
- de overplaatsing;
- het passeren van een periodieke verhoging;
- het intrekken van emolumenten;
- de functieverlaging met de daarbij behorende loonsverlaging;
- vermindering van vakantiedagen;
- schorsing of non-actiefstelling met of zonder behoud van loon;
- het inhouden van het loon;
- de boete¹⁷¹; en
- beëindiging van de arbeidsovereenkomst.

De bovenstaande mogelijkheden die betrekking hebben tot beëindiging van de arbeidsovereenkomst, worden in dit rapport niet verder uiteengezet. Omdat de wettelijke regels hierover door de Wet werk en zekerheid per 1 juli 2015 veranderen en een onderzoek hiertoe voor dit rapport te ver voert.¹⁷² Tevens is uit jurisprudentieonderzoek gebleken dat werkgevers steeds minder vaak de arbeidsovereenkomst wegens overmatig of onbehoorlijk internetgebruik willen beëindigen (zie bijlage 1).

§ 2.6.4.3 Straf of ordemaatregel

Sancties kunnen worden onderverdeeld in straffen en ordemaatregelen, waarbij sommige sancties beide karakters kunnen hebben. Dit onderscheid is van belang, omdat de ene soort sanctie eerder kan worden opgelegd dan de andere en de noodzaak voor het hebben van een grondslag bij beide soorten sancties verschilt.

De sancties die duidelijk worden ingezet om bewust 'leed' toe te voegen en daarnaast de werknemer duidelijk maken dat het overtreden van regels of in strijd handelen met goed werknemerschap niet wordt getolereerd. Deze sancties dienen als 'straf' te worden bestempeld. Sancties die niet als doel hebben om leed toe te voegen, maar om een bepaalde ongewenste situatie te beëindigen zijn een 'ordemaatregel'.¹⁷³

Aan de hand van de omschrijving van de ordemaatregelen, blijkt dat de werkgever bij het opleggen daarvan aan dient te kunnen tonen dat er sprake is van een ongewenste situatie en dat deze maatregel noodzakelijk is ter beëindiging van de ongewenste situatie.

Wanneer de werkgever dit aan kan tonen is daarmee de rechtvaardiging van de ordemaatregel gegeven, omdat het inzetten van de betreffende maatregel immers noodzakelijk is.

Voor straffen die inbreuk maken op de overeengekomen arbeidsvoorwaarden, zoals schorsing zonder behoud van loon, geldt de ongeschreven regel dat daarvoor een contractuele grondslag vereist is. De andere straffen, die dus geen inbreuk maken op de overeengekomen arbeidsvoorwaarden, kunnen op de gezagsverhouding tussen de werkgever en werknemer worden gebaseerd.¹⁷⁴

¹⁷⁰ Koevoets 2006, p. 107: 'De niet-officiële waarschuwing of berisping, die niet in het personeelsdossier wordt opgenomen, is naar de mening van Koevoets en ik deel deze mening geen sanctie, omdat deze maatregelen door de meeste werknemers niet als nadelig wordt beschouwd'.

¹⁷¹ art. 7:650 jo. 7:651 BW.

¹⁷² Kamerstukken I 2013/14, 33 818, A.

¹⁷³ Koevoets 2006, p. 116 en 123-124.

¹⁷⁴ Koevoets 2006, p. 200.

Hieronder zijn nogmaals de sancties, uit subparagraaf 2.6.4.2, weergegeven, maar is nu het onderscheid van straf en ordemaatregel toegepast (zie tabel 1). Daarbij is aangegeven, als er sprake is van een straf, of hier een contractuele grondslag noodzakelijk is door de inbreuk op de overeengekomen arbeidsvoorwaarden.

Sanctie	Straf	Ordemaatregel	Straf? Contractuele grondslag noodzakelijk?
Officiële waarschuwing	X		
Officiële berisping	X		
Overplaatsing	X	X	X
Passeren periodieke verhoging	X		X
Intrekken emolumenten	X		X
Functieverlaging met loonsverlaging	X		X
Vermindering vakantiedagen	X		X
Schorsing/non-actiefstelling zonder behoud van loon	X	X	X
Schorsing/non-actiefstelling met behoud van loon	X	X	
Inhouden van loon	X		X
Boete ¹⁷⁵	X		X

Tabel 1 - Sanctiemogelijkheden onderscheiden in straf en ordemaatregel.

§ 2.6.4.4 Sanctiebeginselen

Bij het opleggen van sancties dient de werkgever met een aantal beginselen rekening te houden. Het eerste beginsel is het 'evenredigheidsbeginsel'. Dit beginsel houdt in dat het gedrag van de werknemer de sanctie moet kunnen rechtvaardigen. Bij het toetsen of hier sprake van is, dient de werkgever bij het opleggen van een sanctie rekening te houden met de aard en de ernst van de fout van de werknemer. Dit houdt in dat de sanctie proportioneel moet zijn. Wanneer dit niet zo is, dan is dit in strijd met goed werkgeverschap en kan de opgelegde sanctie niet worden gerechtvaardigd.¹⁷⁶

Andere beginselen die van belang zijn, het zorgvuldigheidsbeginsel (dat het feitenonderzoek van de werkgever inhoudt), hoor en wederhoor, het maken van een zorgvuldige belangenafweging, het motiveringsbeginsel en het volgen van correcte procedures en in achtname van procedurevoorschriften.¹⁷⁷ Wanneer een werkgever procedurevoorschriften heeft, dan hebben deze volgens de Hoge Raad een belangrijke status.¹⁷⁸ Daarbij dient aan de hand van literatuur te worden opgemerkt, dat het niet naleven van deze procedurevoorschriften bij straffen eerder tot nietigheid leidt dan bij ordemaatregelen.¹⁷⁹

§ 2.6.4.5 Jurisprudentie sancties

Aan de hand van verschillende arbeidsrechtelijke uitspraken die betrekking hebben op overmatig privégebruik of onbehoorlijk gebruik van het internet, is getracht om de belangrijkste uitspraken in de volgende subparagraaf overzichtelijk weer te geven. Bij het opleggen van sancties dient met deze uitspraken rekening te worden gehouden. Hierbij zijn alleen uitspraken vanaf 2002 behandeld, omdat de uitspraken van vóór 2002 inmiddels niet meer relevant zijn. De redenen daarvoor zijn, dat in de literatuur is geschreven dat na het uitbrengen van de eerste versie van het CBP-rapport 'Goed werken in netwerken' in 2001, rechters steeds meer de nadruk zijn gaan leggen op de aanwezigheid van een duidelijk beleid of gedragscode van de werkgever. Daarnaast heeft dit CBP-rapport, zoals eerder aangegeven in paragraaf 2.5, vuistregels gegeven die de

¹⁷⁵ Op grond van artikel 7:650 BW is voor de boete een contractuele grondslag noodzakelijk.

¹⁷⁶ Koevoets 2006, p. 115; Verhulp & Zondag 2008, p. 12.

¹⁷⁷ Verhulp & Zondag 2008, p. 52-53.

¹⁷⁸ HR 9 juli 1990, NJ 1990, 127.

¹⁷⁹ Verhulp & Zondag 2008, p. 52.

werkgever handvatten bieden om een behoorlijk en zorgvuldig beleid vast te stellen op het gebied van controle op internetgebruik.¹⁸⁰ Een andere reden voor de keuze is dat vóór 2002 minder dan 50% van alle Nederlandse huishoudens toegang had tot het internet en aan de hand van de laatste meting door het CBS blijkt dat in 2014 zeker 96% van de Nederlandse huishoudens toegang hebben tot het internet.¹⁸¹ Door dit grote verschil in aansluitingen, de exclusiviteit die daarmee vóór 2002 bestond, is het gebruik van internet in die voorbije jaren veranderd. Dit kan meespelen in de beoordeling door rechters.

Jurisprudentie 2002-2014

Aan de hand van jurisprudentie blijkt dat rechters bij de beoordeling van het opleggen van sancties het in bezit hebben van een gedragscode of reglement dat toeziet op het internetgebruik en de bekendheid daarvan onder de werknemers een grote rol speelt.¹⁸² Het niet hebben van een dergelijke code kan de werkgever worden aangerekend.¹⁸³ Daarnaast is het van belang dat in dit reglement de aard van hetgeen op internet is toegestaan, de duur van het toegestane internetgebruik en de hoogte van de specifieke sancties te benoemen, zodat het opleggen van een sanctie eerder door de rechter wordt geaccepteerd.¹⁸⁴ Wanneer hieraan is voldaan en het reglement dus de mogelijke sanctie(s) benoemt, is het aan de werkgever om te beoordelen of hij de sanctie oplegt.¹⁸⁵ Naast het hebben van een reglement neemt de rechter de mate (frequentie) en aard van het internetgebruik voor privédoeleinden, de diensttijd van de werknemer, de staat van dienst en de invloed dat het internetgebruik op het functioneren van de werknemer heeft gehad mee in zijn beoordeling.¹⁸⁶ Ondanks dat de rechter een reglement van belang acht, moet het voor werknemers in bepaalde situaties ook zonder reglement duidelijk zijn welke handelingen niet zijn toegestaan. Hieronder wordt onder andere het bezoeken van adult en chatsites verstaan.¹⁸⁷ Bij het opleggen van een sanctie dient de werkgever eerst naar andere sancties dan beëindiging van de arbeidsovereenkomst te grijpen.¹⁸⁸ Wanneer de werkgever de arbeidsovereenkomst toch beëindigd of wil beëindigen door de kantonrechter, dient in eerste instantie een waarschuwing te zijn geven. Deze waarschuwing heeft als doel om de werknemer op zijn foutieve gedrag te wijzen, waardoor de werkgever handelt in overeenstemming met het goed werkgeverschap.¹⁸⁹

§ 2.7 Toekomstige veranderingen in het recht op privacy

Binnen de Europese Unie bestaat op nationaal niveau van de verschillende lidstaten nog steeds verschil in de wet- en regelgeving, dat toeziet op de verwerking van persoonsgegevens. Om voor een betere harmonisatie tussen de Europese lidstaten te zorgen, heeft de Europese Commissie voorgesteld om een privacyverordening in te voeren. Deze verordening wordt de Algemene Verordening Gegevensbescherming (afgekort: AVG) genoemd. In 2012 is een voorstel van deze verordening gepubliceerd.¹⁹⁰ Omdat dit een verordening is en een verordening niet omgezet mag worden in nationale wetgeving, voorrang heeft op bestaande en toekomstige nationale rechtsregels en een

¹⁸⁰ Koevoets 2006, p. 193-196.

¹⁸¹ 'Breedbandinternet wint terrein', CBS, www.cbs.nl (zoek op *breedbandinternet huishoudens*) (laatst geraadpleegd op 29 april 2015); 'CBS: Tablet verdringt bord van schoot', CBS, www.cbs.nl (zoek op *internettoegang huishoudens 2014*) (laatst geraadpleegd op 29 april 2015).

¹⁸² Rb. Midden-Nederland (ktr.) 30 april 2014, ECLI:NL:RBMNE:2014:1751, r.o. 4.11.

¹⁸³ Rb. 's-Gravenhage (ktr.) 3 oktober 2002, ECLI:NL:RBSGR:2002:AG7964, r.o. 4.

¹⁸⁴ Rb. 's-Gravenhage (ktr.) 3 oktober 2002, ECLI:NL:RBSGR:2002:AG7964, r.o. 4; Rb. Haarlem (ktr.) 3 april 2003, ECLI:NL:RBHAA:2003:AF7439, r.o. 5.2; Rb. Midden-Nederland (ktr.) 30 april 2014, ECLI:NL:RBMNE:2014:1751, r.o. 4.11.

¹⁸⁵ Rb. Haarlem (ktr.) 15 april 2004, ECLI:NL:RBHAA:2004:AP1254, r.o. 5.3.

¹⁸⁶ Rb. Arnhem (ktr.) 27 maart 2012, ECLI:NL:RBARN:2012:BW0238, r.o. 4.2 en 4.3; Rb. Haarlem (ktr.) 3 april 2003, ECLI:NL:RBHAA:2003:AF7439 r.o. 5.2.

¹⁸⁷ Rb. Haarlem (ktr.) 3 april 2003, ECLI:NL:RBHAA:2003:AF7439 r.o. 5.2, 2.i en 2.j.

¹⁸⁸ Rb. Haarlem (ktr.) 3 april 2003, ECLI:NL:RBHAA:2003:AF7439, r.o. 5.2.

¹⁸⁹ Rb. Maastricht (ktr.) 1 oktober 2009, ECLI:NL:RBMAA:2009:BJ9222; Rb. Midden-Nederland (ktr.) 30 april 2014, ECLI:NL:RBMNE:2014:1751, r.o. 4.12.

¹⁹⁰ Knol e.a. 2013 p. 723-724.

directe werking heeft op het nationale recht van alle Europese lidstaten, zal dit voor meer uniformiteit binnen de Europese Unie zorgen.¹⁹¹ Door de directe verticale en horizontale werking kunnen particulieren de bepalingen uit de verordening, tegen zowel de Europese lidstaten als particulieren bij de nationale rechter inroepen.¹⁹² Deze verordening kent een aantal belangrijke veranderingen of uitbereidingen ten opzichte van de Wbp.

Één wet en één toezichthouder

Een belangrijke en misschien wel dé belangrijkste verandering is, dat voor de hele Europese Unie dezelfde wettelijke regels zullen gaan gelden en de Wbp en andere nationale regelgeving in andere lidstaten zal verdwijnen. Hierdoor zullen ondernemingen die in meerdere Europese lidstaten gevestigd zijn nog maar met één wet rekening hoeven te houden. Daarnaast zullen ondernemingen die in meerdere Europese lidstaten gevestigd zijn, nog maar met één toezichthoudende autoriteit te maken krijgen. Welke toezichthouder bevoegd is hangt af van waar de zogenaamde “belangrijkste vestiging” van de onderneming gevestigd is.¹⁹³

Uitgebreide informatieplicht

De verantwoordelijke heeft de plicht om aan de betrokkene transparant, eenvoudig toegankelijke en begrijpelijke informatie en mededelingen over de verwerking van persoonsgegevens te verschaffen.¹⁹⁴ Zo dient de verantwoordelijke bij de verwerking van persoonsgegevens aan de betrokkene onder andere het doeleinde van de verwerking¹⁹⁵, de periode gedurende welke persoonsgegevens worden opgeslagen¹⁹⁶ en de betrokkene op het recht van rectificatie of het wissen van persoonsgegevens¹⁹⁷ te verstrekken.

Verplichte privacyfunctionaris

Ondernemingen met minimaal 250 werknemers en die persoonsgegevens verwerken, dienen een onafhankelijke functionaris voor gegevensverwerking aan te stellen. In het geval van een groep van ondernemingen kan er één functionaris worden benoemd.¹⁹⁸ Deze functionaris dient door de verantwoordelijke tijdig en naar behoren te worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.¹⁹⁹ De taak van de functionaris is onder andere als contactpunt voor de toezichthoudende autoriteit op te treden en daarnaast de verantwoordelijke te informeren, adviseren en betrokken te zijn bij de beveiliging van persoonsgegevens.²⁰⁰

Privacyeffectbeoordeling

Wanneer de verwerking gezien haar aard, reikwijdte of doeleinden bijzondere risico's inhoudt voor de rechten en vrijheden van betrokkene, dient de verantwoordelijke een beoordeling uit te voeren. Deze beoordeling dient toe te zien op het effect van de beoogde verwerking op de bescherming van persoonsgegevens. Wat deze bijzondere risico's inhouden zijn onder andere de bijzondere persoonsgegevens uit de Wbp. Dit zijn onder andere het seksuele leven, etnische afkomst of systematische en uitgebreide beoordeling van aspecten van de persoonlijkheid van een natuurlijk persoon.²⁰¹

Inwerkingtreding AVG

Over de inwerkingtreding van de AVG bestaat vandaag de dag nog onduidelijkheid. De

¹⁹¹ Opinie 01/2012 Artikel 29-werkgroep, p. 6; Barents 2012, p. 114.

¹⁹² art. 288 VWEU; Kooijmans 2008, p. 270 en 286; Barents 2012, p. 120.

¹⁹³ art. 51 lid 2 jo. 1 onder 13 COM(2012) 11 final.

¹⁹⁴ art. 11 COM(2012) 11 final.

¹⁹⁵ art. 14 lid 1 sub b COM(2012) 11 final.

¹⁹⁶ art. 14 lid 1 sub c COM(2012) 11 final.

¹⁹⁷ art. 14 lid 1 sub d AVG COM(2012) 11 final.

¹⁹⁸ art. 35 lid 1 sub b jo. art. 4 onder 3 jo. 35 lid 2 en art. 36 lid 2 COM(2012) 11 final.

¹⁹⁹ art. 36 lid 1 COM(2012) 11 final.

²⁰⁰ art. 37 lid 1 sub a jo. lid 1 sub b jo. lid 1 sub h COM(2012) 11 final.

²⁰¹ art. 33 lid 1 jo. lid 2 sub a en b COM(2012) 11 final.

recentste ontwikkeling is dat het Voorzitterschap van de Europese Unie een algemene benadering wenst te bereiken tijdens de Raad van Justitie en Binnenlandse Zaken op 15 en 16 juni 2015. Het ziet er naar uit dat deze verordening in 2016 of 2017 inwerking zal treden.²⁰²

§ 2.8 Samenvatting

In dit hoofdstuk is het theoretisch kader omtrent het controleren en sanctioneren van werknemers op internetgebruik uiteengezet.

Werknemers hebben op grond van artikel 8 EVRM en artikel 10 Gw het recht op privacy dat een directe horizontale werking heeft, waardoor de werkgever en de werknemers dit recht ten overstaan van de nationale rechter tegen elkaar in kunnen roepen. Dit privacyrecht geldt op de werkplek van de werknemer, zowel op kantoor als de werkplek thuis, maar ook op de communicatie via het internet. In beginsel mag de werkgever geen inbreuk maken op het recht op privacy. Omdat dit recht niet absoluut is, is rechtmatige beperking mogelijk. De beperking dient dan aan de vereisten in artikel 8 lid 2 EVRM of artikel 10 lid 1 Gw te voldoen. Tevens kan er sprake zijn van een rechtmatige beperking, wanneer de controle op internetgebruik in overeenstemming is met de vereisten uit de Wbp. De Wbp vloeit namelijk voort uit het artikel 10 lid 2 en 3 Gw en dient op grond van jurisprudentie van de Hoge Raad in overeenstemming met artikel 8 EVRM te worden uitgelegd. Om aan de Wbp te kunnen voldoen, dient de controle op het internetgebruik van werknemers onder de reikwijdte van de Wbp te vallen. Er dient sprake te zijn van verwerking van persoonsgegevens. De Wbp zal naar verwachting in 2016 of 2017 verdwijnen. De Wbp wordt dan vervangen door een Europese privacyverordening omtrent de verwerking van persoonsgegevens.

Wanneer er tussen de werkgever en een werknemer een individuele arbeidsovereenkomst tot stand is gekomen, zijn de bepalingen in het arbeidsrecht (Boek 7 Titel 10 BW) van toepassing. Krachtens het arbeidsrecht is de werkgever op grond van de wettelijke instructiebevoegdheid in artikel 7:660 BW en het goed werknemerschap in artikel 7:611 BW, in combinatie met de bijzondere contractuele vertrouwensrelatie tussen de werkgever en werknemer, bevoegd om zijn werknemers bij een vermoeden van overmatig internetgebruik te controleren. Deze werknemer kan voorafgaand aan deze controle op de hoogte zijn gesteld, dit is een open onderzoek. Wanneer de werknemer niet voorafgaand aan de controle op de hoogte is gesteld, is er sprake van een heimelijke controle. Voor deze laatste controle gelden buiten de regels die voor het open onderzoek gelden, nog extra vereisten. Tevens geldt bij de controle op thuiswerkende werknemers als extra vereiste dat er niet mag worden gecontroleerd op internetgebruik, wanneer familieleden ook gebruik mogen maken van de middelen van de werkgever.

Er is sprake van overmatig internetgebruik voor privédoeleinden, wanneer een werknemer aan het internetgebruik voor privédoeleinden buitenproportioneel veel tijd besteed of door dit gebruik de werkzaamheden ernstig ten koste gaan. Twintig uur per week, althans de helft van de werkweek, wordt in de jurisprudentie als excessief beschouwd.

Een werkgever kan op grond van de regels in de individuele of collectieve arbeidsovereenkomst, het instructierecht op basis van de individuele arbeidsovereenkomst en de wettelijke instructiebevoegdheid bevoegd zijn sancties op te leggen. Specifieke wettelijke sancties bij overtreding van internetgebruik bestaan niet, om die reden wordt bij de sanctiemogelijkheden uit het arbeidsrecht, de jurisprudentie en literatuur aangesloten. Daarbij geldt dat niet iedere sanctie zonder contractuele grondslag kan worden opgelegd. Tevens dient bij het opleggen van sancties met verschillende arbeidsrechtelijke sanctiebeginselen rekening te worden gehouden.

In het volgende hoofdstuk wordt de praktijk van Essent aan de hand van de relevante reglementen en interviews uiteengezet.

²⁰² 'E120003', Eerste Kamer, www.eerstekamer.nl (zoek op *Algemene Verordening Privacybescherming*) (laatst geraadpleegd op 5 mei 2015); 'De nieuwe Europese Privacyverordening', ICTRecht, www.ictrecht.nl (zoek op *Europese privacyverordening*) (laatst geraadpleegd op 23 april 2015).

Hoofdstuk 3 Praktijk Essent

§ 3.1 Inleiding

In dit hoofdstuk wordt de praktijk binnen Essent aan de hand van de toepasselijke reglementen van Essent en interviews uiteengezet. Allereerst zal in de tweede paragraaf de arbeidsovereenkomst van Essent worden besproken. Vervolgens worden in de derde paragraaf de bedrijfsmiddelen binnen Essent besproken. In paragraaf vier komt de mogelijkheid tot thuiswerken aan bod. Vervolgens wordt in paragraaf vijf het internet- en controlebeleid van Essent aan de hand van de reglementen en interviews uiteengezet, waarbij het overmatig internetgebruik voor privédoeleinden, de controlemogelijkheden op internetgebruik en de beveiliging van persoonsgegevens met betrekking tot overmatig internetgebruik aan de orde komen. Tot slot worden in paragraaf zes de sanctiemogelijkheden van Essent behandeld.

§ 3.2 Arbeidsovereenkomst

Iedere werknemer binnen Essent heeft een individuele arbeidsovereenkomst waarin de regels zijn opgenomen die de werknemer dient na te leven.²⁰³ De standaard individuele arbeidsovereenkomst van Essent is in bijlage 2 van dit rapport opgenomen. In artikel 9.2 van de individuele arbeidsovereenkomst staat dat de CAO Productie- en Leveringsbedrijven (hierna: CAO PLb), het bedrijfsprotocol en de concernregelingen op de arbeidsovereenkomst van toepassing zijn. Een van deze concernregelingen is de 'Concernregeling nr. 18 Privacyreglement Essent N.V.' (hierna: Privacyreglement). Het bedrijfsprotocol is voor dit onderzoek niet van belang, om die reden zal daar niet verder op worden ingegaan.

§ 3.3 Bedrijfsmiddelen

Werknemers die voor hun werkzaamheden gebruik moeten maken van een laptop, krijgen dit middel in beginsel van Essent. Wanneer een werknemer de voorkeur heeft om van zijn eigen apparatuur, zoals een laptop, gebruik te maken dan is dat mogelijk.²⁰⁴ Dit wordt BYOD (Bring your own device) genoemd.²⁰⁵ In beide gevallen wordt het middel door in te loggen met de gebruikersnaam en het wachtwoord van de werknemer met het(zelfde) bedrijfsnetwerk van Essent verbonden. Dit bedrijfsnetwerk is ook een (bedrijfs)middel die werknemers niet kunnen kiezen. Bij het gebruik van BYOD dienen werknemers de BYOD-gebruikersovereenkomst binnen Essent te ondertekenen.²⁰⁶ In deze overeenkomst zijn geen bepalingen opgenomen die voor dit onderzoek van belang zijn. Om die reden is deze overeenkomst niet als bijlage aan dit rapport toegevoegd.

§ 3.4 Thuiswerken

Werknemers binnen Essent hebben, naast de keuze uit middelen, ook de keuzemogelijkheid om op kantoor of thuis te werken. Deze mogelijkheid bestaat echter alleen bij functies die hiervoor geschikt zijn, bijvoorbeeld kantoorfuncties. Het is aan de werknemer om deze keuze te maken. Zolang de werknemer zijn arbeidsduur nakomt, voldoende "output" levert en eventuele andere afspraken die tussen Essent en de werknemer gelden nakomt.²⁰⁷ Het maakt zowel technisch als theoretisch gezien niets uit waarvandaan een werknemer werkzaam is. In beide gevallen logt een werknemer in op het bedrijfsnetwerk van Essent en vormt dit (op de plaats waarvandaan de werkzaamheden worden verricht na) geen verschil.²⁰⁸

²⁰³ Zie bijlage 5 'Interview M. van Dijk'.

²⁰⁴ Zie bijlage 5 'Interview M. van Dijk'.

²⁰⁵ Dancet e.a. 2013, p. 20.

²⁰⁶ Zie bijlage 5 'Interview M. van Dijk'; Zie bijlage 6 'Interview P. Buijs'.

²⁰⁷ Zie bijlage 5 'Interview M. van Dijk'.

²⁰⁸ Zie bijlage 6 'Interview P. Buijs'.

§ 3.5 Internet- en controlebeleid

Binnen Essent geldt sinds november 2002 het reglement 'Controle op ICT-gebruik' (hierna: ICT-reglement). Dit reglement ziet specifiek toe op het gebruik van e-mail, internet en het bedrijfsnetwerk en de controle daarop.²⁰⁹ Het ICT-reglement is een bijlage van het Privacyreglement dat toeziet op de verwerking van persoonsgegevens binnen Essent.²¹⁰ Het ICT-reglement is in bijlage 3 van dit rapport opgenomen en het Privacyreglement in bijlage 4.

Het ICT-reglement en het Privacyreglement worden hieronder uiteengezet, waarbij de interviews met mevrouw M. van Dijk (manager Industrial Relations en verantwoordelijk voor het Privacyreglement) en de heer P. Buijs (manager Risk Security en verantwoordelijk voor het ICT-reglement) worden betrokken. Het interview met mevrouw M. van Dijk is in bijlage 5 van dit rapport opgenomen en het interview met de heer P. Buijs in bijlage 6. Door zowel gebruik te maken van informatie uit de reglementen en interviews, zorgt dit geheel voor een goed en valide praktijkbeeld over de controle op internetgebruik binnen Essent. Omdat uit beide interviews is gebleken dat de controle op internetgebruik binnen Essent geheel conform de wijze die in het ICT-reglement en het Privacyreglement beschreven staat plaatsvindt, worden deze reglementen als basis voor deze paragraaf gebruikt.²¹¹

§ 3.5.1 Overmatig internetgebruik voor privédoeleinden

Binnen Essent bestaat er geen vaste definitie van het begrip van 'overmatig internetgebruik'. Omdat voor het zakelijk gebruik van internet geen sprake kan zijn van overmatig internetgebruik, wordt hier bij het begrip overmatig internetgebruik voor privédoeleinden aangesloten.²¹²

In het ICT-reglement staat dat het privégebruik van internet de dagelijkse werkzaamheden niet mag storen en geen additionele belasting op het bedrijfsnetwerk mag geven.²¹³ Het is op grond daarvan binnen Essent acceptabel dat iedere werknemer voor privédoeleinden van het internet gebruikmaakt. Uit de interviews blijkt dat de ongeschreven regel is dat een paar minuten per dag gebruik te maken van het internet voor privédoeleinden toegestaan is, maar structureel één uur per dag al snel als overmatig zal worden beschouwd. Daartussenin ligt een groot grijs gebied.²¹⁴

Essent heeft ook geen vaste definitie van het begrip 'privédoeleinden'. Men sluit aan bij de letterlijke betekenis van het woord: het gebruik moet 'privé' zijn. Het dient te gaan om internetgebruik dat slechts voor de werknemer zelf van belang is, dan is er sprake van internetgebruik voor privédoeleinden.²¹⁵

§ 3.5.2 Controle op internetgebruik

Binnen Essent geldt dat de middelen die door Essent voor het verrichten van de werkzaamheden ter beschikking zijn gesteld, primair bedoeld zijn voor zakelijk gebruik. Beperkt privégebruik is daarbij toegestaan, mits dit gebruik de dagelijkse werkzaamheden niet stoort en geen additionele belasting geeft op het bedrijfsnetwerk.²¹⁶

De controle op internetgebruik vindt in overeenstemming met het ICT-reglement plaats. Wanneer zich situaties voordoen waar het ICT-reglement niet in voorziet, zal conform het arbeidsrechtelijke kader, de Wbp en in overleg met de COR worden gehandeld.²¹⁷ Essent

²⁰⁹ art. 1.1 ICT-reglement.

²¹⁰ art. 18.1.2 Privacyreglement; art. 18.3.3.3 sub b Privacyreglement.

²¹¹ Zie bijlage 5 'Interview M. van Dijk'; Zie bijlage 6 'Interview P. Buijs'; art. 1.1 jo. 1.3 ICT-reglement en Inleiding ICT-reglement.

²¹² Zie bijlage 5 'Interview M. van Dijk'; Zie bijlage 6 'Interview P. Buijs'.

²¹³ art. 1.2 ICT-reglement.

²¹⁴ Zie bijlage 5 'Interview M. van Dijk'; Zie bijlage 6 'Interview P. Buijs'.

²¹⁵ Zie bijlage 5 'Interview M. van Dijk'; Zie bijlage 6 'Interview P. Buijs'.

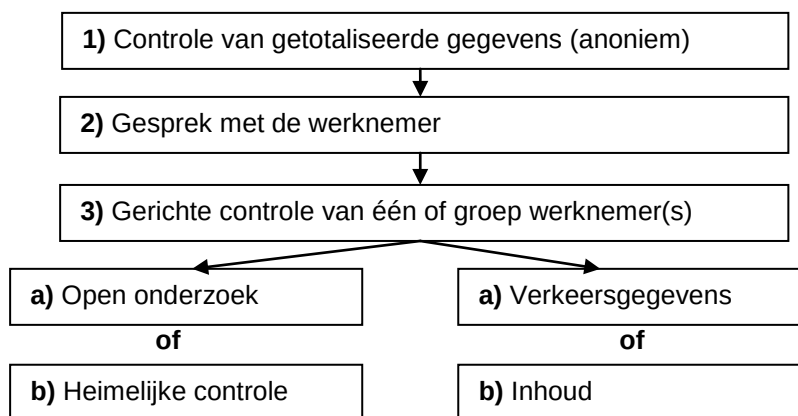
²¹⁶ art. 1.2 ICT-reglement.

²¹⁷ art. 2.1 ICT-reglement.

streeft in beginsel naar een goede balans tussen de controle op verantwoord gebruik van het internet en de bescherming van de privacy van de werknemers op de werkplek.²¹⁸ Wanneer op het internetgebruik van werknemers wordt gecontroleerd, vindt deze controle alleen plaats als er sprake is van een rechtmatige grondslag in de Wbp.²¹⁹ Daarvoor dient minimaal één van de geformuleerde doelen in het ICT-reglement toereikend, ter zake dienend en niet bovenmatig te zijn.²²⁰ Bij de controle op overmatig internetgebruik is het onderstaande geformuleerde doel uit het ICT-reglement van belang:

- de interne controle op het gebruik van bedrijfsmiddelen en bedrijfsbeveiliging.²²¹

Op grond van het bovenstaande doel vindt de controle op overmatig internetgebruik van werknemers plaats. In de meeste gevallen zal er een controle plaatsvinden door een vermoeden of een anonieme tip.²²² In beginsel zal dan een controle plaatsvinden op een niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen.²²³ Indien één of een groep werknemers ervan wordt verdacht de regels te overtreden kan er voor een vastgestelde (korte) periode een gerichte controle plaatsvinden. Voordat deze controle plaatsvindt, zal de leidinggevende eerst een gesprek met de verdachte werknemer aangaan.²²⁴ Door eerst bij de verdachte werknemer zelf te informeren, wordt in lijn met het Privacyreglement gehandeld.²²⁵ Mocht er alsnog gecontroleerd worden, dan zal de verdachte werknemer in beginsel door de leidinggevende voorafgaand aan deze controle op de hoogte worden gesteld van de identiteit van de verantwoordelijke en het doel van deze controle (figuur 1: open onderzoek). Indien het naar het geval niet wenselijk is om de verdachte werknemer voorafgaand aan de controle op de hoogte te stellen, dan kan dit achterwege worden gelaten (figuur 1: heimelijke controle).²²⁶ De gerichte controle vindt in beginsel plaats op verkeersgegevens. Voorbeelden van verkeersgegevens zijn IP-adressen, internetprotocollen, datum en tijd (zie ook paragraaf 2.6.1). Bij zwaarwegende redenen kan de controle ook op de inhoud van het internetgebruik plaatsvinden.²²⁷ Bij een controle op inhoud gaat het voornamelijk om de inhoud van de bezochte internetwebsites en de afbeeldingen die bekeken of gedownload zijn.²²⁸ Een overzicht van de volgorde en de verschillende (controle)mogelijkheden van Essent staan in figuur 1 weergegeven.



Figuur 1 - Volgorde en controle mogelijkheden op internetgebruik door Essent.

²¹⁸ art. 2.2 ICT-reglement.

²¹⁹ art. 18.2.2 Privacyreglement.

²²⁰ art. 18.2.3 sub e Privacyreglement.

²²¹ art. 1.4 punt 1 ICT-reglement.

²²² Zie bijlage 5 'Interview M. van Dijk'; Zie bijlage 6 'Interview P. Buijs'.

²²³ art. 5.2 ICT-reglement.

²²⁴ Zie bijlage 5 'Interview M. van Dijk'; Zie bijlage 6 'Interview P. Buijs'.

²²⁵ art. 18.2.3 sub b Privacyreglement.

²²⁶ art. 5.2 ICT-reglement jo. 18.4.2 Privacyreglement.

²²⁷ art. 5.3 ICT-reglement.

²²⁸ Bijlage 6 'Interview P. Buijs'.

De bevoegde netwerkbeheerder zorgt dat de server de juiste gegevens en de gegevens van de juiste persoon of personen verzameld, die vervolgens in een “logbestand” worden vastgelegd.²²⁹ Het logbestand is naderhand raadpleegbaar door bevoegde personen, zoals netwerkbeheerders die zijn aangewezen in het Privacyreglement.²³⁰ In het geval dat in dit logbestand persoonsgegevens worden opgeslagen, hebben alleen de directeur HR Holding²³¹ en de door hem aangewezen personen toegang tot deze persoonsgegevens.²³² Deze aangewezen personen zijn bevoegd tot het verwerken van deze persoonsgegevens of bevoegd hiervan kennis te nemen.²³³ Tevens mogen deze gegevens niet aan iedereen verstrekt worden. De gegevens kunnen alleen verstrekt worden aan de aangewezen personen en/of bedrijven en alleen voor zover dit noodzakelijk is voor het doeleinde. De specifiek aangewezen personen en/of bedrijven zijn onder andere de betrokkene²³⁴, de netwerkbeheerder²³⁵, de juridische afdeling(en)²³⁶ en de Arbo-dienst²³⁷. Deze personen zijn verplicht tot geheimhouding van de persoonsgegevens, behoudens wettelijk voorschrift of ingeval zij tot mededeling verplicht zijn.²³⁸ Omdat de netwerkbeheerders vaak toegang hebben tot meer of zelfs alle (persoons)gegevens, controleert Essent dit personeel op de integriteit.²³⁹ Wanneer uit de controle blijkt dat de verdachte werknemer zich niet aan de regels houdt, zal de leidinggevende en de betrokken HR-functionaris (in het reglement P&O functionaris genoemd) van de betrokken werknemer zo spoedig mogelijk door de netwerkbeheerder op de hoogte worden gesteld. De leidinggevende zal vervolgens beoordelen of het gebruik gerechtvaardigd is en kan bij overtreding hieraan consequenties verbinden.²⁴⁰

§ 3.5.3 Beveiliging van persoonsgegevens

De persoonsgegevens die uit de verschillende controles op het internetgebruik voortvloeien, worden door Essent niet langer bewaard dan strikt noodzakelijk is voor een verantwoorde uitvoering van de bedrijfsdoelstellingen. De bewaartermijn voor deze gegevens is binnen Essent in beginsel vier weken.²⁴¹ Mocht er bij de controle sprake zijn van verwerking van bijzondere persoonsgegevens, dan worden deze gegevens met in achtneming van de Wbp verwerkt.²⁴²

Essent treft, als verantwoordelijke²⁴³, passende technische en organisatorische maatregelen om verlies en onrechtmatige verwerking van persoonsgegevens tegen te gaan en onnodige verzameling of verdere verwerking te voorkomen. Deze maatregelen zullen een passend beveiligingsniveau garanderen.²⁴⁴ Voor de beveiliging van persoonsgegevens heeft Essent een aantal maatregelen getroffen, waaronder de beveiliging van gebouwen door beveiligingsbedrijven, camera's en toegangssystemen. De serverruimtes zijn tevens afzonderlijk beveiligd met een pasjessysteem en alleen toegankelijk voor netwerkbeheerders. Daarnaast zijn de servers softwarematig met de standaardsysteemsoftware en een extra afzonderlijke beveiligingssoftware beveiligd, waarbij de bestanden die persoonsgegevens bevatten zijn versleuteld. Omdat deze

²²⁹ Zie paragraaf 2.2 voor informatie over het verzamelen van internetgegevens.

²³⁰ art. 18.3.1; Zie bijlage 6 ‘Interview P. Buijs’.

²³¹ art. 18.3.1 sub a jo. 18.1.1 sub k jo. 18.3.2 sub b Privacyreglement.

²³² art. 18.3.1 sub a Privacyreglement.

²³³ art. 18.3.1 sub a jo. 18.1.1 sub l jo. 18.1.1 sub h Privacyreglement.

²³⁴ art. 18.3.2 sub b onder a jo. 18.1.1 sub j Privacyreglement.

²³⁵ art. 18.3.2 sub b onder f jo. 18.1.1 sub n Privacyreglement.

²³⁶ art. 18.3.2 sub b onder i Privacyreglement.

²³⁷ art. 18.3.2 sub b onder l Privacyreglement.

²³⁸ art. 18.3.1 sub b Privacyreglement.

²³⁹ art. 2.4 ICT-reglement; Bijlage 6 ‘Interview P. Buijs’.

²⁴⁰ art. 5.5 ICT-reglement.

²⁴¹ art. 2.3 ICT-reglement jo. 18.2.4 Privacyreglement.

²⁴² art. 18.2.3 sub f Privacyreglement.

²⁴³ art. 18.1.1 sub g Privacyreglement.

²⁴⁴ art. 18.4.1 sub a Privacyreglement.

servers met het bedrijfsnetwerk zijn verbonden, heeft Essent deze servers zowel van binnen als van buiten het bedrijfsnetwerk beveiligd en is het netwerk niet toegankelijk zonder de juiste toegangsgegevens. De afdeling netwerkbeheer zorgt dat de beveiligingssoftware up-to-date blijft en controleert deze periodiek.²⁴⁵ Naast de beveiliging treft de directeur HR Holding de nodige voorzieningen ter bevordering van de juistheid en volledigheid van de persoonsgegevens.²⁴⁶

Iedere werknemer binnen Essent die betrokken is bij de controle op het internetgebruik heeft het recht op informatie, inzage, correctie, alsmede het recht van verzet dat schriftelijk en kosteloos geschied.²⁴⁷

Het ICT-reglement en het Privacyreglement zijn beide gepubliceerd op het intranet van Essent. Hiertoe heeft iedere werknemer toegang.²⁴⁸ Daarnaast heeft Essent de doelen van verwerking en de wijze waarop persoonsgegevens ten hoogste worden verwerkt bij het CBP gemeld.²⁴⁹ Wanneer er in het ICT-reglement of Privacyreglement wijzigingen of aanvullingen worden opgenomen, is dit alleen met instemming van de COR toegestaan.²⁵⁰

§ 3.6 Sancties

In subparagraaf 3.5.2 werd aangegeven dat de leidinggevende van de werknemer die het ICT-reglement overtreedt, daaraan consequenties kan verbinden. Deze consequenties zijn maatregelen die in de CAO PLb 2013-2015 zijn vastgelegd.²⁵¹ Ondanks dat de looptijd van deze CAO PLb verstreken is, heeft de CAO PLb een zogenaamde 'nawerking', waardoor de hieruit voortvloeiende CAO-bepalingen van toepassing zijn.²⁵² Voor dit onderzoek is de theorie over de nawerking verder niet relevant en wordt aangenomen dat de CAO PLb volledig van toepassing is en dus nawerking heeft.

In de CAO PLb staat dat Essent verschillende mogelijkheden heeft om werknemers een 'disciplinaire maatregel', ook wel zoals eerder in subparagraaf 2.6.4.1 besproken een 'sanctie', op te leggen. Voor een eenduidig woordgebruik, wordt hier bij het begrip 'sanctie' aangesloten.

Sancties mogen op grond van de CAO PLb alleen worden opgelegd wanneer een werknemer zijn verplichtingen tegenover de werkgever niet of niet behoorlijk nakomt, of zich niet gedraagt zoals een goed werknemer zich hoort te gedragen.²⁵³ De sancties die op grond van de CAO PLb kunnen worden opgelegd zijn:

- 1) schriftelijke berisping;
- 2) vermindering van verlof van de lopende of daaropvolgende kalenderjaren, van ten hoogste vijf dagen;
- 3) onthouding van periodieke salarisverhoging, voor ten hoogste twee opeenvolgende kalenderjaren;
- 4) terugzetten in lagere functie voor bepaalde tijd of onbepaalde tijd, met of zonder vermindering van salaris;
- 5) overplaatsing;
- 6) schorsing in de uitoefening van de werkzaamheden van de werknemer voor een bepaalde tijd, al dan niet met geheel of gedeeltelijk behoud van salaris.²⁵⁴

²⁴⁵ Zie bijlage 6 'Interview P. Buijs'.

²⁴⁶ art. 18.2.3 sub g Privacyreglement.

²⁴⁷ art. 18.5.1 sub a en 18.5.1 sub b en 18.5.1 sub d Privacyreglement.

²⁴⁸ art. 18.7.2 Privacyreglement; Zie bijlage 5 'Interview M. van Dijk'.

²⁴⁹ art. 18.2.1 jo. 18.6.2 Privacyreglement.

²⁵⁰ art. 18.7.3 jo. 18.1.1 sub c Privacyreglement.

²⁵¹ art. 5.5 ICT-reglement; CAO PLb 2013, p. 55.

²⁵² art. 1.1 CAO PLb 2013; Grinten 2011, p. 33.

²⁵³ art. 19.1 CAO PLb 2013.

²⁵⁴ art. 19.2 lid 1 CAO PLb 2013.

De hierboven onder 2 tot en met 6 genoemde sancties kunnen voorwaardelijk voor een duur van drie jaren worden opgelegd.²⁵⁵ Daarnaast mogen de sancties niet eerder worden opgelegd, dan wanneer de werknemer zich tegenover Essent mondeling of schriftelijk heeft kunnen verantwoorden.²⁵⁶ Tevens dient het opleggen van een sanctie te worden omkleed met redenen²⁵⁷ en is uitvoering van de sanctie mogelijk wanneer de sanctie onherroepelijk is geworden.²⁵⁸

Onverminderd de hierboven genoemde sancties is Essent bevoegd om werknemers voor maximaal één maand in zijn werkzaamheden te schorsen. Dit is mogelijk wanneer een werknemer strafrechtelijk wordt vervolgd wegens een misdrijf. Maar ook wanneer er sprake is van een bijzondere reden waardoor het ongewenst is om de werknemer in zijn functie te houden, nadat zijn arbeidsovereenkomst definitief is beëindigd. Of wanneer de schorsing uit overweging van het bedrijfsbelang noodzakelijk is.²⁵⁹ Deze schorsing kan voortdurend met één maand worden verlengd.²⁶⁰ Voordat Essent kan overgaan tot schorsing van de werknemer, dient Essent de werknemer eerst de gelegenheid te bieden om te worden gehoord, tenzij dat niet mogelijk is.²⁶¹ Wanneer de werknemer alsnog wordt geschorst, blijven de rechten van de werknemer uit de arbeidsovereenkomst in beginsel gehandhaafd.²⁶² Het salaris (plus vaste persoonlijke toeslagen) kan alleen ingeval van een strafrechtelijke vervolging wegens een misdrijf, met ten hoogste een derde deel worden ingehouden.²⁶³

§ 3.7 Samenvatting

In dit hoofdstuk is de praktijk binnen Essent aan de hand van de toepasselijke reglementen en interviews uiteengezet.

Iedere werknemer binnen Essent heeft een individuele arbeidsovereenkomst waarin onder andere de CAO PLb en het Privacyreglement van toepassing zijn verklaard. De bijlage van het Privacyreglement is het ICT-reglement en is daardoor ook van toepassing. Werknemers binnen Essent hebben de keuzemogelijkheid om gebruik te maken van bedrijfsmiddelen van Essent of van henzelf (BYOD). Tevens kunnen werknemers kiezen om op kantoor of thuis te werken. Bij zowel de middelen als de locatie waarvandaan wordt gewerkt, wordt gebruikgemaakt van hetzelfde bedrijfsnetwerk van Essent.

Het Privacyreglement en vooral het ICT-reglement zijn van belang voor de controle op internetgebruik. In het ICT-reglement staat dat de controle op internetgebruik van werknemers in beginsel plaatsvindt op een niveau van getotaliseerde gegevens, die niet herleidbaar zijn tot individuele personen. Vervolgens kan er bij verdenking van één of een groep werknemers die de regels te overtreden gericht op deze werknemers worden gecontroleerd. In beginsel zal Essent eerst een gesprek met de verdachte werknemer aangaan. Mocht er toch een gerichte controle plaatsvinden, dan zal de werknemer in beginsel voorafgaand aan deze controle over de identiteit van de verantwoordelijke en het doel van de controle op de hoogte worden gesteld. In het geval deze mededeling naar aard van het geval niet wenselijk is, dan kan dit volgens het ICT-reglement achterwege worden gelaten. De controle kan zich vervolgens richten op de verkeersgegevens van het internetgebruik, maar ook op de inhoud. Wanneer uit de controle blijkt dat de werknemer overmatig gebruikmaakt van het internet, kunnen hier consequenties aan worden verbonden. De consequenties die Essent kan opleggen zijn in de CAO PLb vastgelegd. In het volgende hoofdstuk wordt het recht uit hoofdstuk twee op de praktijk van Essent uit hoofdstuk drie toegepast.

²⁵⁵ art. 19.2 lid 2 CAO PLb 2013.

²⁵⁶ art. 19.3 lid 1 CAO PLb 2013.

²⁵⁷ art. 19.4 CAO PLb 2013.

²⁵⁸ art. 19.6 CAO PLb 2013.

²⁵⁹ art. 20.1 CAO PLb 2013.

²⁶⁰ art. 20.1 en 20.2 CAO PLb 2013.

²⁶¹ art. 20.2 lid 1 CAO PLb 2013.

²⁶² art. 20.3 lid 1 CAO PLb 2013.

²⁶³ art. 20.3 lid 2 jo. 20.1 lid 1 sub a CAO PLb 2013.

Hoofdstuk 4 Toepassing recht op praktijk Essent

§ 4.1 Inleiding

In dit hoofdstuk wordt de wet- en regelgeving uit hoofdstuk twee op de praktijk binnen Essent uit hoofdstuk drie toegepast. Als eerste wordt in paragraaf twee vastgesteld of Essent bevoegd is tot het controleren van werknemers. Vervolgens wordt in paragraaf drie de controlemogelijkheden op internetgebruik van Essent aan de Wbp getoetst. Verder wordt in paragraaf vier getoetst of Essent mag controleren bij gebruik van BYOD en thuis werkende werknemers. Tot slot wordt in paragraaf vijf de sanctiebevoegdheid en sanctiemogelijkheden van Essent vastgesteld.

§ 4.2 Controlebevoegdheid

Iedere werknemer binnen Essent heeft een individuele arbeidsovereenkomst. Op grond daarvan geldt tussen Essent en de werknemer het arbeidsrecht en de daarbij behorende arbeidsrechtelijke bepalingen. Krachtens deze bepalingen komen Essent als werkgever een aantal bevoegdheden toe, zoals de wettelijke instructiebevoegdheid. Deze bevoegdheid geeft Essent de mogelijkheid om regels op te stellen voor het verrichten van arbeid en het nemen van maatregelen ter bevordering van de goede orde in de onderneming (zie paragraaf 2.6). Van deze bevoegdheid heeft Essent gebruikgemaakt; Essent heeft regels met betrekking tot het internetgebruik in het ICT-reglement vastgelegd (zie paragraaf 3.5). De CAO PLb en het Privacyreglementen, waarvan het ICT-reglement een bijlage is, zijn in de individuele arbeidsovereenkomst van toepassing verklaard (zie paragraaf 3.2 en 3.5). Doordat deze reglementen hierin van toepassing zijn verklaard en de werknemer de individuele arbeidsovereenkomst heeft ondertekend, heeft de werknemer expliciet met deze reglementen ingestemd en is de werknemer gehouden om de regels in de arbeidsovereenkomst en reglementen na te leven (zie paragraaf 2.6). Wanneer wordt vermoed dat een werknemer zich niet aan de regels houdt, is Essent op grond van de wettelijke instructiebevoegdheid en het goed werknemerschap, in combinatie met de bijzondere contractuele vertrouwensrelatie tussen Essent en de werknemer bevoegd tot het controleren op naleving van de regels in het ICT-reglement (zie subparagraaf 2.6.1). Essent is dus bij een vermoeden dat een werknemer zich niet aan de regels houdt bevoegd om op het internetgebruik te controleren. Deze controlebevoegdheid met betrekking tot het internetgebruik heeft Essent in het ICT-reglement vastgelegd (zie subparagraaf 3.5.2). Aan dit reglement dient Essent zich te houden, temeer omdat Essent enkel sancties mag opleggen indien men zich aan de geldende procedurevoorschriften heeft gehouden (zie paragraaf 2.6.4.4).

§ 4.3 Controlemogelijkheden en de Wbp

In het ICT-reglement is de controlebevoegdheid van Essent vastgelegd, waarin de verschillende controlemogelijkheden uiteen zijn gezet (zie paragraaf 3.5). Ondanks dat werknemers het recht op privacy hebben, is dit recht rechtmatig te beperken. Daarvoor dient te worden voldaan aan de vereisten in artikel 8 EVRM, artikel 10 Gw of de Wbp (zie subparagraaf 2.4.2 en 2.4.4).

In beginsel start Essent bij het controleren op internetgebruik met de controle op getotaliseerde gegevens die niet herleidbaar zijn tot een individueel persoon. Hieruit is identificatie van een individueel persoon (redelijkerwijs) onmogelijk, waardoor er geen sprake is van persoonsgegevens en de Wbp op deze controlemogelijkheid niet van toepassing is. Ondanks dat kan Essent rechtmatig gebruikmaken van deze controle op getotaliseerde gegevens, omdat deze mogelijkheid in het ICT-reglement is opgenomen en dit reglement is gepubliceerd op het intranet. Deze controlemogelijkheid is dus bekend bij de werknemers binnen Essent en hebben de werknemers daardoor geen redelijke verwachting tot privacy. Het recht op privacy is om die redenen op grond van het arrest Halford tegen Verenigd Koninkrijk en artikel 8 lid 2 EVRM rechtmatig beperkt. In vervolg hierop kan een gerichte controle op het internetgebruik van deze werknemer plaatsvinden.

Gerichte (open onderzoek of heimelijke) controle

Bij een gerichte controle op één of een groep werknemers wordt niet gecontroleerd op grond van een vermoeden, maar op grond van een verdenking. Dit houdt in dat er meer moet dan een vermoeden van overmatig internetgebruik voor privédoeleinden aanwezig moet zijn. De verdachte werknemer wordt in beginsel voorafgaand aan de controle door de leidinggevende over de identiteit van Essent en het doel van deze controle op de hoogte gesteld. Omdat de werknemer in beginsel voorafgaand aan de controle hiervan op de hoogte wordt gesteld en de controlebevoegdheid in het ICT-reglement is opgenomen, is er sprake van een open onderzoek (zie subparagraaf 2.6.1). Wanneer het naar de aard van het geval niet wenselijk is om de werknemer voorafgaand aan de gerichte controle op de hoogte te stellen, wordt de gerichte controle zonder voorafgaande mededeling uitgevoerd. Ondanks dat Essent deze controlemogelijkheid in het ICT-reglement heeft opgenomen, is er sprake van een heimelijke controle (zie subparagraaf 2.6.1).

Controle op verkeersgegevens of inhoud

De gerichte controle kan vervolgens op verkeersgegevens en inhoud plaatsvinden. In beginsel vindt de controle op verkeersgegevens plaats, maar bij zwaarwegende redenen kan dit ook op inhoud plaatsvinden. Omdat in de meeste situaties geen sprake zal zijn van zwaarwegende redenen, vindt deze controle in beginsel alleen op verkeersgegevens plaats. Volledigheidshalve wordt de controle op inhoud in de volgende subparagrafen meegenomen.

§ 4.3.1 Toetsing aan reikwijdte Wbp

In de voorgaande paragraaf is ingegaan op de wijze waarop Essent controles uitvoert. In deze paragraaf zal stapsgewijs worden bekeken in hoeverre die controles voldoen aan de eisen van de Wbp. De belangrijkste vereisten uit de Wbp, die in hoofdstuk twee zijn behandeld, vormen daarbij het uitgangspunt.

Persoonsgegevens

De gerichte controle richt zich specifiek op één of een groep vooraf bepaalde verdachte werknemers. Daardoor worden alleen de verkeersgegevens van deze werknemer(s) verzameld en vastgelegd. De inhoud van de vastgelegde verkeersgegevens geven informatie over het internetgebruik en de werknemer, bijvoorbeeld IP-adres, internetprotocol, datum en tijd. Aan de hand van deze gegevens kan de werknemer (een natuurlijk persoon) redelijkerwijs gemakkelijk (indirect) worden geïdentificeerd. Wanneer de controle op inhoud plaatsvindt, wordt naar de inhoud van de verzamelde gegevens gekeken. Deze gegevens geven informatie over bijvoorbeeld de bezochte internetwebsites en afbeeldingen die door de werknemer zijn gedownload. Aan de hand van deze gegevens is het, net zoals bij verkeersgegevens, mogelijk om een werknemer (direct of indirect) te identificeren en is dit in sommige gevallen wellicht zelfs eenvoudiger. Bij zowel het verzamelen van verkeersgegevens als verzamelen van gegevens voor de controle op inhoud, is op grond van artikel 1 sub a Wbp sprake van persoonsgegevens.

Geautomatiseerde verwerking van persoonsgegevens

De verkeersgegevens en de gegevens voor de controle op inhoud, worden door een server van Essent verzameld, vastgelegd en uiteindelijk vernietigd. Deze gegevens kunnen naderhand (voordat deze zijn vernietigd) door de aangewezen personen worden geraadpleegd. In beginsel is dit de netwerkbeheerder. Omdat deze gegevens naderhand raadpleegbaar zijn, is er sprake van een feitelijke macht over deze gegevens. Er is dus op grond van artikel 1 sub b Wbp sprake van een verwerking van persoonsgegevens. Omdat deze verwerking softwarematig en op aanwijzing van de netwerkbeheerder plaatsvindt, is er op grond van artikel 1 sub b juncto 2 lid 1 Wbp sprake van een gedeeltelijk geautomatiseerde verwerking van persoonsgegevens.

Verantwoordelijke

Essent is een in Nederland gevestigde rechtspersoon, die al sinds 1999 onder deze naam

energie opwekt en verkoopt aan particulieren en ondernemingen. Om die reden is er in Nederland een economische activiteit in de zin van de Wbp aanwezig. Essent heeft het doel voor de controle op internetgebruik in het ICT-reglement vastgelegd en de server voor de verwerking van persoonsgegevens in eigendom en eigenbeheer. Essent is op grond daarvan en het feit dat Essent zichzelf als ‘verantwoordelijke’ in het Privacyreglement aanwijst, verantwoordelijke in de zin van artikel 4 lid 1 juncto 1 sub d Wbp. Essent is daardoor verantwoordelijk voor de naleving van de Wbp.

§ 4.3.2 Toepassing Wbp

Ingevolge van de toetsing in subparagraaf 4.3.1, dient de gerichte controle op verkeersgegevens of inhoud, dat zowel een open onderzoek of heimelijke controle kan zijn, ook rechtmatig te zijn. Of er sprake is van een rechtmatige controle (verwerking van persoonsgegevens) door Essent zal deze subparagraaf uitwijzen.

Doeleinden

De controle op internetgebruik mag op grond van de Wbp alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden uitgevoerd. Essent heeft de doeleinden op basis waarvan de controle plaatsvindt, voorafgaand aan een eventuele controle in het ICT-reglement omschreven en vastgelegd. Het doeleinde dat voor de controle op internetgebruik van belang is, is het doel: ‘de interne controle op het gebruik van bedrijfsmiddelen en bedrijfsbeveiliging’. Dit doel is duidelijk omschreven en mag in redelijkheid worden verwacht dat een ieder dit begrijpt. Toch is dit doel redelijk ruim omschreven, omdat het begrip “bedrijfsmiddelen” een redelijke ruime betekenis kan hebben en de betekenis van dit begrip niet in het ICT-reglement is omschreven. Essent kan op grond hiervan al redelijk snel overgaan tot controle op verschillende middelen, dat kan zorgen voor onduidelijkheid onder de werknemers. Ondanks de ruime betekenis van het begrip, is het doel niet dermate ruim geformuleerd en wordt voldaan aan artikel 7 Wbp. Dit doel dient vervolgens in alle stadia van de verwerking gerechtvaardigd te zijn. Daarvoor dient aan één van de in artikel 8 Wbp opgesomde rechtmatigheidsgrondslagen worden voldaan.

Rechtmatigheidsgrondslagen

Voordat kan worden bepaald of de controle op internetgebruik in alle stadia van de controle gerechtvaardigd is, dient aansluiting te worden gezocht bij één van de opgesomde rechtmatigheidsgrondslagen in artikel 8 sub a tot en met f Wbp. De rechtmatigheidsgrondslag die voor de gerichte controle op internetgebruik van toepassing is, is artikel 8 sub f Wbp. Om aan deze rechtmatigheidsgrondslag te voldoen, dient de verwerking van persoonsgegevens (de controle op het internetgebruik) voor Essent noodzakelijk te zijn voor de behartiging van het gerechtvaardigde belang van Essent. Wanneer hieraan is voldaan dient op grond van de Hoge Raad aan de vereisten van proportionaliteit en subsidiariteit uit artikel 8 lid 2 EVRM te worden voldaan.

In paragraaf 4.2 is uiteengezet dat Essent op grond van het arbeidsrecht en de daaruit voortvloeiende bevoegdheden, bevoegd is om bij een vermoeden dat een werknemer zich niet aan de regels houdt te controleren. Op grond van deze bevoegdheid en de omstandigheid dat Essent de gerichte controle op grond van ICT-reglement alleen bij een verdenking (en dus meer dan een vermoeden) uitvoert handelt Essent rechtmatig. Het belang dat Essent bij de controle op internetgebruik heeft, is dat werknemers de overeengekomen arbeidsduur voldoende productief vervullen en er voor Essent geen extra kosten ontstaan of tijdverlies optreedt. Dit specifieke belang is voor Essent van grote waarde, omdat het personeelsbestand door de huidige economische situatie van Essent gedwongen slinkt. Daarnaast dienen werknemers de regels met betrekking tot het internetgebruik na te leven en dienen ze zich als goed werknemers te gedragen. Aan de hand van deze toetsing is er sprake van een gerechtvaardigd belang. De gerichte controle aan de hand van een open onderzoek is dus gerechtvaardigd. Dit geldt niet voor een heimelijke controle; ondanks dat het overmatig internetgebruik voor privédoeleinden

wel een verboden handeling is op grond van het ICT-reglement, is er geen sprake van een strafbare handeling of zwaarwegend belang. Het belang van een groot bedrijf als Essent, dat betrekking heeft op het tegengaan van extra kosten (economisch belang) of tijdverlies, weegt niet op tegen het recht op privacy van de individuele werknemer. Daarnaast dienen alle mogelijkheden te zijn uitgeput, dus ook de mogelijkheid van een open onderzoek. Daarbij komt dat het vereiste in het ICT-reglement voor de heimelijke controle onjuist is. In dit reglement staat het vereiste: “de aard van het geval niet wenselijk is”. De gerichte heimelijke controle is dus niet gerechtvaardigd.

Naast het feit dat er voor een open onderzoek naar internetgebruik een gerechtvaardigd belang aanwezig is, dient dit belang ook noodzakelijk te zijn. Daarvoor dient het belang van Essent tegen het belang van de verdachte werknemer een zelfstandig gewicht te krijgen. Het belang van deze werknemer dient door de rechtsverhouding (afhankelijke positie) tussen Essent en de werknemer een zwaarder gewicht te krijgen. Voor een juiste afweging van de noodzakelijke eis dienen de onderstaande vragen gemotiveerd te worden beantwoord en het zelfstandige gewicht van het belang van de werknemer daarin te worden betrokken:

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

In het onderhavige geval is het belang van Essent, zoals hiervoor al is beschreven, dat voor Essent geen extra kosten ontstaan of tijdverlies plaatsvindt.

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?

Door op het internetgebruik van een werknemer te controleren wordt er inbreuk gemaakt op de persoonlijke levenssfeer, het recht op privacy, van de werknemer uit artikel 8 lid 1 EVRM en artikel 10 lid 1 Gw. Hoewel deze inbreuk wordt gemaakt, wordt de inbreuk geminimaliseerd tot alleen de verdachte werknemers en zijn er verschillende andere maatregelen genomen. Zoals in beginsel alleen op verkeersgegevens te controleren, zo kort mogelijke periode te controleren en wordt de werknemer voorafgaand aan de controle op de hoogte gesteld van de identiteit van Essent en het doel van de controle. Door in beginsel alleen op verkeersgegevens te controleren en de controleperiode te beperken, wordt in overeenstemming met de regels van het CBP gehandeld. Daarnaast treft Essent organisatorische en systematische beveiligingsmaatregelen, zoals beveiliging van de server, het aanwijzen van personen die toegang hebben tot de verzamelde persoonsgegevens en de geheimhoudingsplicht voor deze personen. Door alleen op deze selecte groep van verdachte werknemers te controleren, in beginsel alleen op verkeersgegevens te controleren en de toegang tot de persoonsgegevens te beperken tot een selecte groep, wordt de inbreuk op het recht op privacy dusdanig beperkt dat de gegevensverwerking (controle op het internetgebruik) door Essent niet achterwege moet blijven. Essent voldoet daarmee aan de Wbp.

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

Het doel dat Essent met de controle op het internetgebruik nastreeft, is om verdachte werknemers te controleren op het gebruik van bedrijfsmiddelen. Werknemers mogen gebruikmaken van bedrijfsmiddelen, zoals het internet, maar dit gebruik mag niet leiden tot verstoring van de dagelijkse werkzaamheden of tot additionele belasting voor het bedrijfsnetwerk van Essent. Andere mogelijkheden om dit doel te bereiken zijn bijvoorbeeld de controle op output van de verdachte

werknemer of het registreren van inlogtijden op het bedrijfsnetwerk. Deze mogelijkheden zijn niet ter zake dienend, omdat iedere werknemer een ander werktempo heeft, ander takenpakket heeft, vaker dan de ander kan worden gestoord of gewoonweg het bijhouden van inlogtijden niets zegt over het internetgebruik van de werknemer. Daarom kan het doel niet langs andere weg (zonder verwerking) op een valide manier worden bereikt. De controle op internetgebruik is daarmee in overeenstemming met de Wbp en in overeenstemming met het subsidiariteitsbeginsel van artikel 8 lid 2 EVRM.

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

De gerichte controle op internetgebruik wordt alleen uitgevoerd in overeenstemming met het ICT-reglement. Hierdoor wordt deze controle alleen uitgevoerd wanneer een werknemer wordt verdacht de regels te overtreden. De werknemer wordt voorafgaand aan dit open onderzoek op de hoogte gesteld van de identiteit van Essent en het doel van de controle, de controle vindt in beginsel zo kort mogelijk en in beginsel alleen op verkeersgegevens plaats. De inbreuk op het recht op privacy wordt dus geminimaliseerd en evenredig tot het doel. Hierdoor wordt proportioneel en in overeenstemming met de Wbp gehandeld.

Op grond van deze toetsing voldoet alleen de gerichte controle door Essent in de vorm van een open onderzoek op internetgebruik aan de rechtmatigheidsgrondslag uit artikel 8 sub f Wbp. Die zowel op verkeersgegevens als bij zwaarwegende redenen op inhoud kan plaatsvinden.

Bijzondere persoonsgegevens

Bij een controle op internetgebruik, waarbij alleen wordt gecontroleerd op verkeersgegevens, is geen sprake van bijzondere persoonsgegevens in de zin van artikel 16 e.v. Wbp. Bij de controle op inhoud is het op voorhand niet helder of er bijzondere persoonsgegevens worden verwerkt. Mocht het zo zijn dat bij deze inhoudscontrole bijzondere persoonsgegevens aan het licht komen, dan zal Essent deze gegevens met inachtneming van de Wbp verwerken. Daarmee voldoet Essent aan de artikelen 16 e.v. Wbp.

Voordat de verwerking van persoonsgegevens rechtmatig is, dient Essent aan de overige verplichtingen te voldoen (zie subparagraaf 2.5.5.4 t/m 2.5.5.8).

Verwerking verenigbaar met het doel

Essent gebruikt de verkregen persoonsgegevens bij de controle op het internetgebruik alleen voor het doeleinde waarvoor zij verzameld zijn. Dit is voor de controle op het gebruik van bedrijfsmiddelen en bedrijfsbeveiliging. Door deze gegevens alleen voor dit doeleinde te gebruiken wordt voldaan aan het verenigbaar gebruik in artikel 9 Wbp.

Maatregelen

Essent heeft verschillende maatregelen getroffen om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. Bij het verzamelen van gegevens wordt door Essent geen onnodige informatie verzameld, omdat de server alleen de gegevens verzameld die ter zake dienend zijn om te beoordelen of er sprake is van overmatig internetgebruik voor privédoeleinden. Deze persoonsgegevens worden vervolgens beveiligd en versleuteld op de server opgeslagen. Hiermee voldoet Essent aan artikel 11 Wbp. Daarnaast treft Essent technische en organisatorische beveiligingsmaatregelen om verlies en onrechtmatige verwerking tegen te gaan. Als eerste heeft Essent in het ICT-reglement personen aangewezen die toegang hebben tot de persoonsgegevens, die tevens gehouden zijn aan een geheimhoudingsplicht. Vervolgens zijn de persoonsgegevens softwarematig beveiligd en versleuteld, is het gebouw en de ruimte waar de server staat beveiligd door een beveiligingsbedrijf en een pasjessysteem. Door

deze genomen maatregelen hebben alleen bevoegde personen toegang tot dit gebouw, de serverruimte en daarmee de persoonsgegevens. Hierbij moet overigens worden opgemerkt dat een 100%-beveiliging nooit mogelijk. Essent heeft daarmee voldoende passende maatregelen genomen en voldoet het aan de geheimhoudingsplicht in artikel 12 Wbp en de passende beveiligingseis in artikel 13 Wbp.

Overige verplichtingen

De persoonsgegevens die Essent bij het uitvoeren van een gerichte controle verzamelt, worden niet langer bewaard dan strikt noodzakelijk is voor een verantwoorde bedrijfsdoelstelling. Dit is binnen Essent in beginsel vier weken. Hiermee wordt voldaan aan het vereiste in artikel 10 lid 1 Wbp en wordt de maximumtermijn van zes maanden uit het artikel 32 lid 6 Vrijstellingsbesluit Wbp niet overschreden. Omdat Essent in het ICT-reglement de mogelijkheid heeft opgenomen om werknemers heimelijk op internetgebruik te controleren, dient Essent te voldoen aan de meldingsplicht in de Wbp. Essent houdt zich aan deze meldingsplicht en is daarmee voldaan aan artikel 27 lid 1 Wbp.

Uit de bovenstaande toetsing is gebleken dat een controle op getotaliseerde gegevens niet onder de reikwijdte van de Wbp valt, maar op grond van artikel 8 lid 2 EVRM het recht op privacy rechtmatig beperkt. Alleen de gerichte controle op internetgebruik van één of een groep verdachte werknemers is in de vorm van een open onderzoek rechtmatig op grond van de Wbp. Deze controle dient zich in beginsel alleen te richten op de verkeersgegevens en bij zwaarwegende redenen is de controle op inhoud rechtmatig. Doordat is voldaan aan de Wbp, is daarmee ook voldaan aan artikel 8 EVRM en artikel 10 Gw. Er is dus sprake van een rechtmatige verwerking van persoonsgegevens in de zin van artikel 6 Wbp en wordt het recht op privacy rechtmatig beperkt. Eveneens is uit deze toetsing gebleken dat het ICT-reglement in grote lijnen, behalve de heimelijke controle, voldoet aan de Wbp en andere grondrechten.

§ 4.4 Controle bij BYOD en thuiswerken

Het is van belang om te toetsen of er een verschil bestaat voor de rechtmatigheid van het controleren op internetgebruik bij het gebruik van BYOD en thuiswerken (zie paragraaf 3.3 en 3.4).

Bij zowel het gebruik van middelen van Essent als eigen middelen (BYOD) wordt er door werknemers op het bedrijfsnetwerk van Essent ingelogd en gebruikgemaakt van het bedrijfsnetwerk van Essent. Omdat de controle op internetgebruik door en op de server van Essent wordt uitgevoerd, wordt er dus geen enkele controle op het middel van de werknemer uitgevoerd. Om die reden maakt het dus geen verschil of men van eigen middelen, of bedrijfsmiddelen gebruikmaakt.

In het ICT-reglement staat dat het bedrijfsnetwerk en het daarmee verbonden internet door werknemers beperkt voor privédoeleinden gebruikt mag worden, zolang dit gebruik de dagelijkse werkzaamheden niet stoort en geen additionele belasting geeft op het bedrijfsnetwerk (zie subparagraaf 3.5.1). Werknemers die op kantoor of vanuit huis werken, werken zoals eerder in paragraaf 3.4 aangegeven beide op hetzelfde bedrijfsnetwerk van Essent. Omdat de controle op internetgebruik, zoals eerder in deze paragraaf aangegeven, op de server van Essent plaatsvindt, bestaat er geen enkel verschil in de controle op werknemers op kantoor of thuis. In het ICT-reglement is geen bepaling opgenomen waarin staat dat familieleden via het bedrijfsnetwerk van Essent geen gebruik mogen maken van het internet. Het is om die reden bij een thuiswerkende werknemer op voorhand niet duidelijk of de werknemer, een familielid of een ander persoon gebruikmaakt van het internet. Omdat tussen Essent en een familielid of een ander persoon geen arbeidsrechtelijke relatie bestaat, kan Essent in dat geval geen beroep doen op de arbeidsrechtelijke bepalingen. Daardoor kan er niet met zekerheid worden gezegd of Essent de controlebevoegdheid heeft om rechtmatig op het internetgebruik van de thuiswerkende werknemers te controleren. Om die reden dient de controle bij de thuiswerkende werknemers achterwege te worden gelaten en kan alleen

op het internetgebruik van de werknemer op kantoor worden gecontroleerd (zie paragraaf 2.6.1).

§ 4.5 Sanctiemogelijkheden

In paragraaf 4.2 is aangegeven dat iedere werknemer een individuele arbeidsovereenkomst heeft, waarin de regels in de CAO PLb, het Privacyreglement en het ICT-reglement van toepassing zijn verklaard. Wanneer een werknemer de regels die hierin staan overtreedt, zoals overmatig internetgebruik voor privédoeleinden, is Essent op grond van de regels in de individuele arbeidsovereenkomst in combinatie met het ICT-reglement, het instructierecht en de wettelijke instructiebevoegdheid bevoegd sancties op te leggen. De sancties die bij overmatig internetgebruik voor privédoeleinden kunnen worden opgelegd staan in de CAO PLb (paragraaf 3.6). Omdat niet iedere sanctie zonder een contractuele grondslag mag worden opgelegd, is hiervan in subparagraaf 2.6.4.3 (zie tabel 1) een overzicht gemaakt. Dat overzicht is toegepast en vergeleken met de sancties in de CAO PLb. Uit deze vergelijking is de onderstaande tabel voortgekomen (zie tabel 2). In deze tabel staan de sancties die Essent op grond van het arbeidsrecht of de CAO PLb kan opleggen.

Sanctie	Arbeidsrecht	CAO PLb
Officiële waarschuwing	X	
Officiële berisping	X	X
Overplaatsing (straf)		X
Overplaatsing (ordemaatregel)	X	
Passeren van periodieke verhoging		X
Functieverlaging met loonsverlaging		X
Vermindering vakantiedagen		X
Schorsing/non-actiestelling met behoud van loon (ordemaatregel)	X	
Schorsing/non-actiestelling met behoud van loon (straf)	X	X
Schorsing/non-actiestelling zonder behoud van loon (ordemaatregel)	X	
Schorsing/non-actiestelling zonder behoud van loon (straf)		X

Tabel 2 - Sanctiemogelijkheden Essent o.g.v. het arbeidsrecht en de CAO.

Bij het opleggen van een van de in tabel 2 genoemde sancties dient Essent de sanctiebeginselen toe te passen. In eerste instantie dient er in overeenstemming met het evenredigheidsbeginsel te worden gehandeld, waarbij Essent rekening dient te houden met de aard en de ernst van de overtreding. Inhoudende dat de sanctie proportioneel moet zijn, zodat de sanctie gerechtvaardigd is. Daarnaast dient er rekening te worden gehouden met het zorgvuldigheidsbeginsel en het maken van een zorgvuldige belangenafweging (zie subparagraaf 2.6.4.4). Op grond van de CAO PLb dient Essent ook rekening te houden met de mondelinge of schriftelijke verantwoording van de werknemer, de motivering van de sanctie en mag de sanctie worden uitgevoerd wanneer deze onherroepelijk is geworden (zie paragraaf 3.6). Bovendien is het van belang om in overeenstemming met de jurisprudentie te handelen (zie subparagraaf 2.6.4.5). Hieruit vloeit voort dat het opleggen van een sanctie bij overmatig internetgebruik voor privédoeleinden niet snel door de rechter zal worden geaccepteerd. Omdat Essent in het ICT-reglement niet exact de duur van het toegestane internetgebruik voor privédoeleinden heeft benoemd en bij overtreding daarvan alleen naar de sancties uit de CAO PLb verwijst. Bij het opleggen van de sanctie dient rekening te worden gehouden met de mate, aard en invloed van het internetgebruik, de diensttijd en staat van dienst van de werknemer. Waarbij beëindigen van de individuele arbeidsovereenkomst als laatste middel moet worden gezien en voorafgaand hieraan altijd een waarschuwing moet zijn gegeven. Omdat de feiten in iedere situatie verschillend zijn en de feiten in de afweging een ander gewicht kunnen hebben, is het ingewikkeld om op voorhand te bepalen welke sanctie het meest geschikt is. Dit dient aan de hand van de vereisten per situatie te worden bepaald. Duidelijk is in ieder geval dat Essent verschillende

sanctiemogelijkheden heeft en het begrip “internetgebruik voor privédoeleinden” nog specifiek en exacter in het ICT-reglement moet worden omschreven.

§ 4.6 Samenvatting

In dit hoofdstuk is de wet- en regelgeving op de praktijk binnen Essent toegepast. Iedere werknemer binnen Essent heeft een individuele arbeidsovereenkomst, waarin de CAO PLb, het Privacyreglement en het ICT-reglement als bijlage van het Privacyreglement van toepassing zijn verklaard. Werknemers zijn gehouden deze reglementen na te leven. Op grond van de arbeidsovereenkomst geldt tussen Essent en de werknemer het arbeidsrecht en de daarbij behorende arbeidsrechtelijke bepalingen. Op grond van deze arbeidsrechtelijke bepalingen komt Essent de wettelijke instructiebevoegdheid en het goed werknemerschap toe. Deze bepalingen in combinatie met de bijzondere contractuele vertrouwensrelatie tussen Essent en de werknemer brengen met zich mee, dat Essent bevoegd is om bij een vermoeden van overmatig internetgebruik voor privédoeleinden hierop een controle uit te voeren. Deze controlebevoegdheid heeft Essent in het ICT-reglement vastgelegd. De eerste controlemogelijkheid is de controle op getotaliseerde gegevens. Hierop is de Wbp niet van toepassing, omdat het (redelijkerwijs) onmogelijk is om uit deze gegevens een individuele persoon te identificeren. Deze mogelijkheid kan rechtmatig worden ingezet, omdat onder de werknemers geen sprake is van een redelijke verwachting tot privacy en daarmee wordt voldaan aan artikel 8 lid 2 EVRM. Naast deze controlemogelijkheid heeft Essent de mogelijkheid om bij een verdenking van overmatig internetgebruik voor privédoeleinden door een werknemer gericht te controleren. Deze gerichte controle kan in de vorm van een open onderzoek of een heimelijke controle plaatsvinden, waarbij in beginsel wordt gecontroleerd op verkeersgegevens en bij zwaarwegende redenen ook op de inhoud van het internetgebruik. Bij een controle op internetgebruik is niet snel sprake van zwaarwegende redenen, waardoor deze controle in beginsel alleen op verkeersgegevens zal plaatsvinden. Bij het gericht controleren is de Wbp van toepassing, omdat er sprake is van verwerking van persoonsgegevens. Essent wordt hierin als verantwoordelijke gezien, waardoor Essent gehouden is de Wbp na te leven. De gerichte controle kan niet rechtmatig in de vorm van een heimelijk onderzoek worden uitgevoerd, omdat Essent geen zwaarwegend belang heeft, en niet alle mogelijkheden zijn uitgeput, zoals de mogelijkheid van een open onderzoek. Het belang van Essent is niet zwaarwegend omdat het belang van het tegengaan van extra kosten of tijdverslies niet zwaarder weegt dan het recht op privacy van de individuele werknemer. In het ICT-reglement staat dat een heimelijke controle mogelijk is als aan het vereiste: “de aard van het geval niet wenselijk is” is voldaan. Dit is onjuist, er dient sprake te zijn van een “zwaarwegend belang” en verdenking van strafbare of verboden handelingen. Essent voldoet met de gerichte controle op internetgebruik in de vorm van een open onderzoek wel aan de rechtmatigheidsgrondslag en andere vereisten uit de Wbp. Daarmee wordt ook in overeenstemming met artikel 8 EVRM en artikel 10 Gw gehandeld. Essent is bevoegd een controle op internetgebruik op zowel op apparatuur van Essent, als dat van de werknemer zelf (BYOD) uit te voeren. Hierbij dient Essent er rekening mee te houden dat de controle alleen mag worden uitgevoerd bij werknemers die op kantoor zijn. Dit omdat bij een thuiswerksituatie op voorhand niet duidelijk is welke persoon of personen gebruikmaken van het internet. Hierdoor ontstaat onduidelijkheid over de arbeidsrechtelijke relatie en de controlebevoegdheid die Essent op grond daarvan heeft. Essent is op grond van de regels in de individuele arbeidsovereenkomst in combinatie met het ICT-reglement, het instructierecht en de wettelijke instructiebevoegdheid bevoegd sancties op te leggen. De sancties die bij overmatig internetgebruik opgelegd kunnen worden zijn arbeidsrechtelijke sancties of sancties uit de CAO PLb. Bij het opleggen van deze sancties dient Essent rekening te houden, met de contractuele grondslag, de sanctiebeginselen uit het arbeidsrecht en de CAO PLb en dient er in overeenstemming met de jurisprudentie te worden gehandeld. In het volgende hoofdstuk komen de conclusies en aanbevelingen aan bod.

Hoofdstuk 5 Conclusies en aanbevelingen

§ 5.1 Inleiding

In dit hoofdstuk wordt antwoord gegeven op de centrale vraag die aan dit onderzoek ten grondslag ligt. De centrale vraag luidt als volgt: 'In hoeverre mag Essent zijn werknemers, gelet op de huidige wet- en regelgeving en de privacyregels van Essent, controleren op overmatig internetgebruik en bij overtreding daarvan sanctioneren?'. Deze vraag zal in de volgende twee paragrafen worden beantwoord. In de eerste paragraaf komen de belangrijkste conclusies aan de orde en tot slot zullen er aanbevelingen worden gegeven.

§ 5.2 Conclusies

De huidige technische ontwikkelingen en toenemende mogelijkheden op het internet, hebben het voor werknemers interessanter en makkelijker gemaakt om tijdens werktijd gebruik te maken van het internet. Omdat veel werknemers thuiswerken is het voor Essent steeds moeilijker om dit internetgebruik te controleren. Dit was voor Essent de aanleiding om een onderzoek uit te laten voeren naar de controlebevoegdheid en controlemogelijkheden die Essent heeft op het internetgebruik van werknemers. En of Essent bevoegd is zijn werknemers sancties op te leggen, indien er sprake is van overmatig internetgebruik voor privédoeleinden en welke sanctiemogelijkheden Essent hiervoor heeft.

Recht op privacy

Werknemers hebben op grond van artikel 8 EVRM en artikel 10 Gw het recht op privacy. Dit recht kan de werknemer ten overstaan van een nationale rechter tegen de werkgever inroepen. Het recht op privacy geldt niet alleen op de werkplek op kantoor, maar ook op de werkplek thuis en de communicatie via het internet. In beginsel mag Essent geen inbreuk maken op dit recht, maar kan dit toch rechtmatig worden beperkt. Beperking is mogelijk door aan de vereisten in artikel 8 lid 2 EVRM of artikel 10 lid 1 Gw te voldoen, maar ook door in overeenstemming met de Wbp te handelen. De Wbp vloeit namelijk voort uit artikel 10 lid 2 en 3 Gw en dient volgens de Hoge Raad in overeenstemming met artikel 8 EVRM te worden uitgelegd. Voor een geslaagd beroep op de Wbp dient de controle op internetgebruik onder de reikwijdte van Wbp te vallen.

Controlebevoegdheid

Iedere werknemer binnen Essent heeft een individuele arbeidsovereenkomst. Op grond van die arbeidsovereenkomst zijn de arbeidsrechtelijke bepalingen in Boek 7 Titel 10 BW van toepassing op Essent en de werknemer. Krachtens deze arbeidsrechtelijke bepalingen is Essent op grond van de wettelijke instructiebevoegdheid (art. 7:660 BW), het goed werknemerschap (art. 7:611 BW), in combinatie met de contractuele vertrouwensrelatie tussen Essent en de werknemer bevoegd om zijn werknemers bij een vermoeden van overtreding van de geldende regels te controleren. Dit geldt ook bij overmatig internetgebruik voor privédoeleinden. Essent heeft de controlebevoegdheid met betrekking tot internetgebruik in het eigen ICT-reglement vastgelegd.

Soorten controles

In beginsel dient Essent volgens dit ICT-reglement te controleren op getotaliseerde gegevens, waaruit identificatie van een persoon (redelijkerwijs) onmogelijk is. Hierdoor is de Wbp niet van toepassing op deze vorm van controleren. Door deze controle in het ICT-reglement te hebben opgenomen is het recht op privacy op grond van artikel 8 EVRM wel rechtmatig beperkt.

Wanneer één of een groep werknemers wordt verdacht van overmatig internetgebruik voor privédoeleinden, kan Essent de verdachte werknemer gericht controleren op internetgebruik. Deze gerichte controle dient in beginsel kort te worden uitgevoerd en zal zich in beginsel richten op de verkeersgegevens, zoals het IP-adres, de tijd en de datum. Bij zwaarwegende redenen kan Essent ook op de inhoud van het internetgebruik

controleren. Bij de gerichte controle is er sprake van verwerking van persoonsgegevens, waardoor de Wbp hierop van toepassing is. Daarnaast dient Essent als verantwoordelijke zorg te dragen voor de naleving van de Wbp. Uit de toetsing aan de Wbp is gebleken dat Essent rechtmatig gericht op verkeersgegevens kan controleren. Deze gerichte controle is bij zwaarwegende redenen ook op inhoud mogelijk. Hiervan zal in de meeste situaties bij internetgebruik geen sprake zijn.

Open onderzoek of heimelijke controle

De gerichte controle wordt in beginsel als een open onderzoek uitgevoerd. De verdachte werknemer wordt voorafgaand aan de controle op de hoogte gesteld van de identiteit van Essent en het doel van de controle. Wanneer alle andere middelen, zoals een open onderzoek zijn ingezet, kan deze mededeling achterwege worden gelaten. Dan dient er sprake voor Essent sprake te zijn van een zwaarwegend belang en verboden of strafbare handelingen. Deze controle wordt een heimelijke controle genoemd. Een heimelijke controle is bij een controle op overmatig internetgebruik voor privédoeleinden niet mogelijk, ondanks dat het overmatige internetgebruik voor privédoeleinden een verboden handeling is. Omdat het belang van een groot bedrijf als Essent, het belang om kosten en tijdverslies tegen te gaan, niet opweegt tegen het recht op privacy van de individuele werknemer is een heimelijke controle niet gerechtvaardigd en dus niet rechtmatig. Essent kan dus alleen rechtmatig gericht controleren, in de vorm van een open onderzoek, dat in beginsel alleen is gericht op verkeersgegevens.

Binnen Essent hebben werknemers de keuzemogelijkheid om gebruik te maken van eigen middelen (BYOD) of middelen van Essent. Met beide middelen wordt er ingelogd op het(zelfde) bedrijfsnetwerk van Essent. Omdat de controle op het internetgebruik op de server van Essent plaatsvindt, maakt het gebruikte middel niets uit voor de controle. Daarnaast mogen werknemers binnen Essent kiezen om op kantoor of thuis te werken. Wanneer er wordt gecontroleerd op het internetgebruik, dient Essent rekening te houden dat alleen mag worden gecontroleerd, wanneer de werknemer op kantoor aanwezig is. Dit vanwege het feit dat op voorhand niet duidelijk is welke persoon of personen thuis gebruikmaken van het internet. Hierdoor bestaat er onduidelijkheid of de arbeidsrelatie aanwezig is en daarmee ook de controlebevoegdheid van Essent.

Overmatig internetgebruik voor privédoeleinden

Werknemers mogen van Essent beperkt gebruik maken van het internet voor privédoeleinden, zolang dit de dagelijkse werkzaamheden niet stoort en geen additionele belasting geeft op het bedrijfsnetwerk van Essent. Er is volgens jurisprudentie sprake van overmatig internetgebruik voor privédoeleinden, wanneer aan het internetgebruik buitenproportioneel veel tijd wordt besteed of wanneer dit gebruik ernstig ten koste gaat van de werkzaamheden. Twintig uur of de helft van de werkweek wordt in jurisprudentie als excessief beschouwd.

Sanctiebevoegdheid en mogelijkheden

Op grond van het arbeidsrecht is Essent bevoegd tot het opleggen van sancties. De mogelijke sancties zijn gebaseerd op het arbeidsrecht en de CAO Productie- en Leveringsbedrijven (hierna: CAO PLb). Dit zijn:

- de officiële waarschuwing;
- de officiële berisping;
- de overplaatsing;
- het passeren van periodieke verhoging;
- de vermindering van vakantiedagen;
- de schorsing/non-actiestelling met en zonder behoud van loon.

Bij het opleggen van deze sancties dient Essent rekening te houden met een aantal sanctiebeginselen uit het arbeidsrecht, de CAO PLb en de jurisprudentie. Het is op

voorhand niet duidelijk welke sanctie bij het overmatig internetgebruik voor privédoeleinden geschikt is, dit dient per situatie te worden bekeken.

Concluderend uit het bovenstaande is Essent bevoegd om zijn werknemers te controleren, mits er sprake is van een vermoeden van overmatig internetgebruik voor privédoeleinden. Er is sprake van overmatig internetgebruik wanneer de werknemer buitenproportioneel veel tijd aan het internetgebruik voor privédoeleinden besteed of de werkzaamheden ernstig ten koste gaan door dit gebruik.

Wanneer er alleen sprake is van een vermoeden, is Essent bevoegd om rechtmatig te controleren op getotaliseerde gegevens waaruit identificatie van een persoon (redelijkerwijs) onmogelijk is. Wanneer er sprake is van een verdenking van overmatig internetgebruik voor privédoeleinden, dan is een gerichte controle in de vorm van een open onderzoek ook rechtmatig. Deze gerichte controle dient zich in beginsel alleen op verkeersgegevens te richten. Essent mag de twee bovengenoemde controlemogelijkheden mogen door alleen uitvoeren wanneer de werknemer op kantoor aanwezig is.

Komt uit de controle naar voren dat de werknemer overmatig gebruik heeft gemaakt van het internet voor privédoeleinden, dan is Essent bevoegd deze werknemer een passende sanctie uit het arbeidsrecht of de CAO PLb op te leggen.

§ 5.3 Aanbevelingen

Naar aanleiding van de bovenstaande conclusies volgen in deze paragraaf concrete aanbevelingen.

Aangepast ICT-reglement

Het ICT-reglement dient naar aanleiding van het onderzoek op een aantal punten te worden aangepast. Deze punten zijn in een nieuw ICT-reglement in bijlage 7 van dit rapport opgenomen. De belangrijkste veranderingen zijn de volgende toevoegingen:

- a) alleen werknemers mogen gebruik maken van het internet en familie dus niet meer, waardoor controle tijdens thuiswerken mogelijk wordt gemaakt (artikel 2 in het nieuwe ICT-reglement);
- b) overmatig internetgebruik voor privédoeleinden valt onder het 'verboden gebruik' (artikel 5 lid 1 sub b jo. 6 lid 1 sub h in het nieuwe ICT-reglement);
- c) wanneer is er sprake van overmatig internetgebruik voor privédoeleinden, zodat werknemers duidelijker voor ogen hebben wat wel en niet toegestaan is (artikel 6 lid 2 in het nieuwe ICT-reglement);
- d) bij de eis voor een heimelijke controle, dat er sprake dient te zijn van een zwaarwegend belang en strafbare of verboden handeling die door de werknemer(s) worden verricht (artikel 7 lid 2 in het nieuwe ICT-reglement)

Privacyverordening

In 2016 of 2017 zal de nieuwe Europese verordening omtrent de verwerking van persoonsgegevens inwerking treden, waardoor Essent of RWE onder andere een privacyfunctionaris zal moeten aanstellen. Ook zal het privacyreglement daarop moten worden aangepast. Aanbevolen wordt om een vervolgonderzoek naar deze verordening uit te voeren, wanneer de verordening daadwerkelijk inwerking treedt en dus de inhoud van die verordening vaststaat. Aan de hand van de uitkomst van dit onderzoek dient het ICT-reglement te worden aangepast.

Privé- en werktijd

Aanbevolen wordt om een vervolgonderzoek uit te voeren naar de privé- en werktijd, zodat Essent deze tijd beter kan afbakenen. De uitkomst van dit onderzoek dient vervolgens in het ICT-reglement te worden opgenomen. Voor Essent en de werknemers is dan duidelijk wanneer sprake is van privé- en werktijd en kan het registreren van privéhandelingen in privétijd door dit onderscheid zoveel mogelijk worden vermeden.

Literatuurlijst/bronvermelding

Handboeken

Barents 2012

R. Barents, *Europees recht*, Groningen: Noordhoff Uitgevers 2012.

Berkvens e.a. 2007

J.M.A. Berkvens, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2007.

Blokker e.a. 2014

N.M. Blokker e.a., *Vijftig juridische opstellen voor een Leidse nachtwacht*, 's-Gravenhage: Boom Juridische Uitgevers 2014.

Borking 2010

J.J.F.M. Borking, *Recht en praktijk: Privacyrecht is code*, Deventer: Kluwer 2010.

Bunschoten 2010

D.E. Bunschoten, *Tekst & Commentaar artikel 10 Grondwet*, Deventer: Kluwer 2010 (online, laatst bijgewerkt op 1 september 2009) .

Dancet e.a. 2013

L. Dancet e.a., *Privacy Deskundig en praktisch juridisch advies*, Eindhoven: Ius Mentis 2013.

Grinten 2011

W.H.A.C.M. Bouwens & R.A.A. Duk, *Arbeidsovereenkomstenrecht*, Deventer: Kluwer 2011.

Helm 2009

I. van der Helm, *Monografieën Sociaal Recht: De privacybescherming van de zieke werknemer*, Deventer: Kluwer 2009.

Henrard 2006

K. Henrard, *Mensenrechten vanuit internationaal en nationaal perspectief*, 's-Gravenhage: Boom Juridische uitgevers 2006.

Hof e.a. 2014

S. van der Hof e.a., *Recht en Praktijk: Recht en computer*, Deventer: Kluwer 2014.

Hooghiemstra e.a. 2013

T.F.M. Hooghiemstra, *SDU Commentaar Wet bescherming persoonsgegevens*, 's-Gravenhage: Sdu Uitgevers 2013.

Huydecoper 2006

S.M. Huydecoper, *Wet Bescherming Persoonsgegevens en ICT*, 's-Gravenhage: Sdu Uitgevers 2006.

Knol e.a. 2013

P.C. Knol e.a., *Tekst & Commentaar Telecommunicatie- en privacyrecht*, Deventer: Kluwer 2013.

Kooijmans 2008

P.H. Kooijmans, *Internationaal publiekrecht in Vogelvlucht*, Deventer: Kluwer 2008.

Kranenborg & Verhey 2011

H.R. Kranenborg & L.F.M. Verhey, *Mastermonografieën: Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011.

Schaaik 2011

G.A.F.M. van Schaaik, *Praktijkgericht juridisch onderzoek*, 's-Gravenhage: Boom Juridische uitgevers 2011.

Verhulp & Zondag 2008

E. Verhulp & W.A. Zondag, *Monografieën Sociaal Recht: Disfunctioneren en wangedrag van werknemers*, Deventer: Kluwer 2008.

Vries & Rutgers 2001

H.H. de Vries & D.J. Rutgers, *Actualiteiten Sociaal Recht: Wet bescherming persoonsgegevens Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001.

Vaktijdschriften

Vries, Van der Jagt & Roosendaal 2008

H.H. de Vries, F.C. van der Jagt & A.P.C. Roosendaal, *Module Privacy en persoonsgegevens 219: Controle door de werkgever*, Deventer: Kluwer (online, laatst bijgewerkt op 26 juni 2008).

Rapporten

Koevoets 2006

M.M. Koevoets, *Wangedrag van werknemers* (diss. Rotterdam Erasmus Universiteit), 's-Gravenhage: Boom Juridische Uitgevers 2006.

Opinie 01/2012 Artikel 29-werkgroep

Artikel 29-werkgroep, *Opinion 01/2012 - 00530/12/EN WP 191*, Brussel: Artikel 29-werkgroep 2012.

Opinie 06/2014 Artikel 29-werkgroep

Artikel 29-werkgroep, *Opinion 06/2014 - 844/14/EN WP 217*, Brussel: Artikel 29-werkgroep 2014

Rapport CBP Publicatie van persoonsgegevens op internet 2007

CBP, *Richtsnoeren CBP 'Publicatie van persoonsgegevens op internet*, 's-Gravenhage: CBP 2007.

Rapport CBS ICT kennis en economie 2014

CBS, *ICT kennis en economie*, 's-Gravenhage: CBS 2014.

Rapport Staatscommissie Grondwet 2010

Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 's-Gravenhage: Staatscommissie Grondwet 2010.

Rapport TNS NIPO Media Standaard Survey 2013

TNS NIPO, *Rapportage 2013 Media Standaard Survey (MSS)*, Amsterdam: TNS NIPO 2014.

Sauerwein & Linnemann 2002

L.B. Sauerwein & J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens*, 's-Gravenhage: Ministerie van Justitie 2002.

Terstegge 2002

J.H.J. Terstegge, *Goed werken in netwerk - Regels voor controle op e-mail en internetgebruik van werknemers*, 's-Gravenhage: Sdu Uitgevers 2002.

Winter e.a. 2008

H.B. Winter e.a., *Wat niet weet, wat niet deert*, 's-Gravenhage: Wetschappelijk Onderzoek- en Documentatiecentrum 2008.

Elektronische bronnen

'Artikel 1 sub a Wbp', CBP, cbpweb.nl (zoek op *artikel 1 sub a persoonsgegevens*) (laatst geraadpleegd op 23 april 2015).

'Artikel 11 lid 1 Wbp', CBP, cbpweb.nl (zoek op *artikel 11 lid 1*) (laatst geraadpleegd op 1 mei 2015).

'Artikel 11 lid 2 Wbp', CBP, cbpweb.nl (zoek op *artikel 11 lid 2*) (laatst geraadpleegd op 1 mei 2015).

'Artikel 27 lid 1 Wbp', CBP, cbpweb.nl (zoek op *artikel 27 lid 1*) (laatst geraadpleegd op 1 mei 2015).

'Artikel 29-werkgroep', CBP, cbpweb.nl (zoek op *EDPS*) (laatst geraadpleegd op 9 mei 2015).

'Artikel 4 lid 1 Wbp', CBP, cbpweb.nl (zoek op *artikel 4 lid 1 verantwoordelijke*) (laatst geraadpleegd op 28 april 2015).

'Artikel 6 Wbp', CBP, cbpweb.nl (zoek op *artikel 6*) (laatst geraadpleegd op 29 april 2015).

'Artikel 7 Wbp', CBP, cbpweb.nl (zoek op *artikel 7*) (laatst geraadpleegd op 29 april 2015).

'Breedbandinternet wint terrein', CBS, www.cbs.nl (zoek op *breedbandinternet huishoudens*) (laatst geraadpleegd op 29 april 2015).

'CBP legt Google sanctie op voor privacyschendende voorwaarden', CBP, www.cbp.nl (zoek op *privacy Google*) (laatst geraadpleegd op 31 maart 2015).

'CBP onderzoekt nieuwe privacyvoorwaarden Facebook', CBP, www.cbp.nl (zoek op *privacyvoorwaarden Facebook*) (laatst geraadpleegd op 31 maart 2015).

'CBS: Tablet verdringt bord van schoot', CBS, www.cbs.nl (zoek op *internettoegang huishoudens 2014*) (laatst geraadpleegd op 29 april 2015).

'Controle van personeel', CBP, cbpweb.nl (zoek op *heimelijke controle*) (laatst geraadpleegd op 19 mei 2015).

'De nieuwe Europese Privacyverordening', ICTRecht, www.ictrecht.nl (zoek op *Europese privacyverordening*) (laatst geraadpleegd op 23 april 2015).

'E120003', Eerste Kamer, www.eerstekamer.nl (zoek op *Algemene Verordening Privacybescherming*) (laatst geraadpleegd op 5 mei 2015).

'Over RWE', Essent, www.essent.nl (zoek op *RWE*) (laatst geraadpleegd op 31 maart 2015).

'Privé, Van Dale, www.vandale.nl (zoek op *privé*) (laatst geraadpleegd op 25 april 2015).

'Profiel', Essent, www.essent.nl (zoek op *profiel Essent*) (laatst geraadpleegd op 31 maart 2015).

'Sanctie', Van Dale, www.vandale.nl (zoek op *sanctie*) (laatst geraadpleegd op 24 april 2015).

'Verdragen en wetten', College voor de rechten van de mens, www.mensenrechten.nl (zoek op *ratificeren EVRM*) (laatst geraadpleegd op 23 april 2015).

'Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden', Nederlandse overheid, overheid.nl (zoek op *EVRM*) (laatst geraadpleegd op 23 april 2015)

'Wet bescherming persoonsgegevens', CBP, www.cpbweb.nl (zoek op *Wet bescherming persoonsgegevens*) (laatst geraadpleegd op 1 mei 2015).

Jurisprudentie

EHRM 16 december 1992, NJ 1993, 400, m.nt. E.J. Dommering (*Niemietz/Bondsrepubliek Duitsland*).

EHRM 25 juni 1997, 173/1996, NJ 1998, 506, m.nt. P.J. Boon (*Halford/Verenigd Koninkrijk*).

EHRM 7 november 2002, 58341/00 (*Madsen/Denemarken*).

EHRM 9 maart 2004, 46210/99 (*Wretlund/Zweden*).

EHRM 3 april 2007, 62617/00, NJ 2007, 617, m.nt. E.J. Dommering (*Copland/Verenigd Koninkrijk*).

HvJ EG 13 november 1990, C-106/89 (*Marleasing*).

HvJ EU 15 januari 2014, C-176/12 (*Laboubi*).

HvJ EU 17 december 2014, C-582/14 (*Breyer/Bondsrepubliek Duitsland*).

HR 9 januari 1987, ECLI:NL:HR:1987:AG5500.

HR 9 juli 1990, NJ 1990, 127.

HR 8 april 1994, ECLI:NL:HR:1994:ZC1322.

HR 27 april 2001, ECLI:NL:HR:2001:AB1347.

HR 31 mei 2002, ECLI:NL:PHR:2002:AD9609.

HR 13 juni 2011, ECLI:NL:PHR:2011:BQ8097.

HR 9 september 2011, ECLI:NL:HR:2011:BQ8097.

CRvB 28 augustus 2014, ECLI:NL:CRVB:2014:2974.

Gerechtshof Amsterdam 18 juli 2002, ECLI:NL:GHAMS:2002:AE5514.

Rb. 's-Gravenhage (ktr.) 3 oktober 2002, ECLI:NL:RBSGR:2002:AG7964.

Rb. Haarlem (ktr.) 3 april 2003, ECLI:NL:RBHAA:2003:AF7439.

Rb. Haarlem (ktr.) 15 april 2004, ECLI:RBHAA:2004:AP1254.

Rb. Dordrecht 31 augustus 2004, ECLI:NL:RBDOR:2004:AR5275.

Rb. Maastricht (ktr.) 1 oktober 2009, ECLI:NL:RBMAA:2009:BJ9222

Rb. Arnhem (ktr.) 27 maart 2012, ECLI:NL:RBARN:2012:BW0238.

Rb. Oost-Nederland (zittingplaats Almelo) 21 maart 2013, ECLI:NL:RBONE:2013:BZ5412.

Rb. Midden-Nederland (ktr.) 30 april 2014, ECLI:NL:RBMNE:2014:1751.

Europese stukken

Verordening (EG) 45/2001.

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

COM(2012) 11 final.

Parlementaire stukken

Kamerstukken II 1975/76, 13 872, 3 (MvT).

Kamerstukken II 1997/98, 25 892, 3 (MvT).

Kamerstukken I 2013/14, 33 818, A.

Trb. 1951, 154.

Stb. 2001, 250.