

Controle op de werknemer

De controle- en sanctiemogelijkheden
van de werkgever bij overmatig internetgebruik

BIJLAGEN

Auteur:	Sven van der Meer
Opdrachtgever:	Essent N.V.
Plaats en datum:	's-Hertogenbosch, 28 mei 2015

Bijlagen

De bijlagen in dit document behoren bij de afstudeerscriptie 'Controle op de werknemer, de controle- en sanctiemogelijkheden van de werkgever bij overmatig internetgebruik'. De paginanummering verschilt met de nummering in de afstudeerscriptie.

Inhoudsopgave

Bijlagen.....	1
Bijlage 1 - Jurisprudentieoverzicht 2000-2014	3
Bijlage 2 - Standaard arbeidsovereenkomst Essent	5
Bijlage 3 - Reglement Essent Controle op het ICT-gebruik.....	9
Bijlage 4 - Concernregeling Privacyreglement Essent	13
Bijlage 5 - Interview M. van Dijk.....	19
Bijlage 6 - Interview P. Buijs	21
Bijlage 7 - Nieuw ICT-reglement.....	25

Bijlage 1 Jurisprudentieoverzicht 2000-2014

In deze bijlage wordt de jurisprudentie met betrekking tot het beëindigen van de arbeidsovereenkomst wegens overmatig of onbehoorlijk internetgebruik van het jaar 2000 tot en met het jaar 2014 opgesomd. Deze opsomming vormt de basis voor grafiek 1 op de volgende pagina. Getracht is om alle jurisprudentie in de vorm van ECLI weer te geven, dit is niet in alle gevallen mogelijk gebleken.

2000

- Rb. Rotterdam (ktr.) 10 april 2000, ECLI:NLLKTGROT:2000:AG5321.
- Rb. Haarlem (ktr.) 16 juni 2000, ECLI:NL:KTGHAA:2000:AG5277.
- Rb. Utrecht (ktr.) 13 juli 2000, ECLI:NL:KTGUTR:2000:AG5335.
- Rb. Apeldoorn (ktr.) 6 september 2000, ECLI:NL:KTGAPD:AJ0147.
- Rb. Hilversum (ktr.) 6 september 2000, ECLI:NL:KTGHIL:2000:AG2607.
- Rb. Utrecht (ktr.) 20 november 2000, ECLI:NL:KTGUTR:2000:AA8947.
- Rb. Utrecht (ktr.) 20 november 2000, JAR 2001,1.
- Rb. Emmen (ktr.) 29 november 2000, JAR 2001, 4.

2001

- Rb. Amsterdam (ktr.) 26 april 2001, ECLI:NL:KTRAMS:2001:AG2741.
- Rb. Sittard (ktr.) 3 december 2001, ECLI:NL:KTGSIT:2001:AG7843.
- Rb. Maastricht (ktr.) 3 december 2001, ECLI:NL:RBMAA:2001:AD8224.
- Rb. Sittard (ktr.) 21 december 2001, ECLI:NL:KTGSIT:2001:AF9912.

2002

- Rb. Amsterdam (ktr.) 19 april 2002, ECLI:NL:RBAMS:2002:AG7844.
- Rb. Alkmaar (ktr.) 27 juni 2002, ECLI:RBALK:2002:AG7892.
- Rb. 's-Gravenhage (ktr.) 3 oktober 2002, ECLI:NL:RBSGR:2002:AG7964.

2003

- Rb. Haarlem (ktr.) 3 april 2003, ECLI:NL:RBHAA:2003:AF7439.
- Rb. Breda (ktr.) 12 juni 2003, ECLI:NL:RBBRE:2003:AO0120.
- Rb. Roermond (ktr.) 27 juni 2003, ECLI:NL:RBROE:2003:AO0118.

2004

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

2005

- Rb. Amsterdam (ktr.) 17 juni 2005, ECLI:NL:RBAMS:2005:AU0832.
- Rb. Haarlem (ktr.) 4 augustus 2005, ECLI:NL:RBHAA:2005:AU2880.

2006

- Rb. Amsterdam (ktr.) 20 juni 2006, ECLI:NL:RBAMS:2006:BG0313.

2007

- Rb. Breda (ktr.) 4 april 2007, ECLI:NL:RBBRE:2007:BA5352.

2009

- Rb. Haarlem (ktr.) 1 september 2009, ECLI:NL:RBHAA:2009:BJ7362.
- Rb. Maastricht (ktr.) 1 oktober 2009, ECLI:NL:RBMAA:2009:BJ9222.

2011

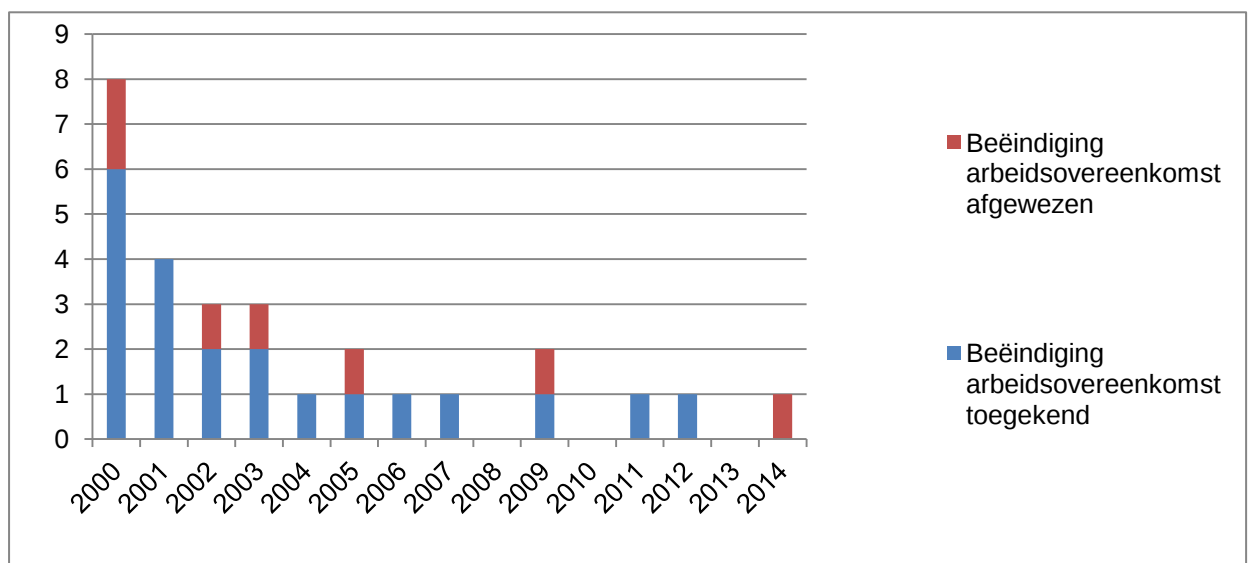
- Rb. Rotterdam (ktr.) 21 september 2011, ECLI:NL:RBROT:2011:BU4848.

2012

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

2014

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



Grafiek 1 - Jurisprudentie m.b.t. beëindigen arbeidsovereenkomst door internetgebruik in periode 2000-2014.

Bijlage 2 Standaard arbeidsovereenkomst Essent

ARBEIDSOVEREENKOMST

Ondergetekenden:

Essent Personeel Service B.V., statutair gevestigd te Arnhem en kantoorhoudende te 's-Hertogenbosch, hierbij rechtsgeldig vertegenwoordigd door mevrouw <<naam>>, directeur Essent Service, hierna te noemen "de werkgever",

en

«de heer/mevrouw» «Naam werknemer», geboren op «geboortedatum» te «geboorteplaats», wonende aan «straatnaam», «postcode» te «postcode en woonplaats», hierna te noemen "de werknemer",

(waar in deze overeenkomst met betrekking tot personen wordt gesproken over werknemer, hij, hem of zijn worden daarmee zowel mannelijke als vrouwelijke personen aangeduid),

verklaren een arbeidsovereenkomst te zijn aangegaan onder de volgende voorwaarden en bedingen:

Artikel 1 Datum indiensttreding, functie en standplaats

1.1

Werknemer treedt met ingang van «datum» in dienst van de werkgever in de functie van «functiebenaming» bij de Business Unit «BY», afdeling «afdeling», subafdeling <subafdeling>.

1.2

Bij het aangaan van de arbeidsovereenkomst is de standplaats «plaats».

Artikel 2 Duur van de overeenkomst, proeftijd en tussentijdse opzegging

2.1

Deze arbeidsovereenkomst wordt aangegaan voor onbepaalde tijd.

2.2

De eerste <<twee maanden/maand>> na aanvang van de arbeidsovereenkomst <<gelden/geld>> als proeftijd. Gedurende de proeftijd heeft ieder der partijen de bevoegdheid de arbeidsovereenkomst met onmiddellijke ingang op te zeggen.

2.3

Onverminderd het bepaalde in lid 1 en lid 2 van dit artikel, kan ieder der partijen de overeenkomst tussentijds opzeggen met inachtneming van de wettelijke opzegtermijn.

Artikel 3 Salaris en arbeidsvoorwaardelijke regelingen

3.1

Het salaris bedraagt bij het aangaan van de arbeidsovereenkomst € «bedrag» bruto per maand op basis van salarisklasse «klasse» en op basis van bovengenoemde de in artikel 4 genoemde 40-urige werkweek.

3.2

De vakantie-uitkering bedraagt 8% van het in de maand geldende salaris, voor elke periode waarin de werknemer aanspraak heeft op salaris. De vakantie-uitkering wordt maandelijks aan de werknemer toegekend in het benefit budget.

3.3

Het salarisoverzicht wordt maandelijks digitaal aan de werknemer beschikbaar gesteld.

Artikel 4 Arbeidsduur en werktijden

Fulltime:

De gemiddelde arbeidsduur op basis van 100% bedraagt 38 uur per week. Dit wordt gerealiseerd door 40 uur per week te werken en 104 ADV-uren per jaar in te roosteren.

Parttime:

De gemiddelde arbeidsduur op basis van 100% bedraagt 38 uur per week. Dit wordt gerealiseerd door 40 uur per week te werken en 104 ADV-uren per jaar in te roosteren. Omdat werknemer voor «percentage»% werkzaam is, bedraagt de gemiddelde arbeidsduur per week «aantal uren» uur inclusief een naar rato toekenning van het aantal ADV-uren. Het rooster wordt na overleg met de werknemer door werkgever vastgesteld.

Artikel 5 Geheimhouding

5.1

Werknemer is verplicht tot geheimhouding van gegevens zowel tijdens als na dienstverband, die door werkgever (waaronder voor het doel van dit artikel tevens is begrepen de Business Unit waar werknemer is tewerk gesteld) als vertrouwelijk zijn aangemerkt of waarvan werknemer het vertrouwelijke karakter kan vermoeden.

5.2

Werknemer mag ter beschikking staande/gestelde klantgegevens:

- alleen gebruiken voor de uitvoering van de door werkgever opgedragen werkzaamheden; en
- alleen ter beschikking stellen aan de door werkgever aangewezen functionarissen en/of afdelingen.

Artikel 6 Documenten

Het is de werknemer verboden op welke wijze dan ook documenten en/of correspondentie en/of andere informatiedragers en/of kopieën hiervan, die aan de werkgever toebehoren, in zijn/haar bezit te houden, uitgezonderd voorzover en voor zolang dit voor de uitoefening van zijn/haar werkzaamheden voor de werkgever is vereist. In ieder geval is de werknemer verplicht om, zelfs zonder enig verzoek daartoe, dergelijke documenten en/of correspondentie en/of andere informatiedragers en/of kopieën hiervan aan het einde van de arbeidsovereenkomst, ofwel bij non-activiteit om welke reden dan ook, onmiddellijk aan de werkgever ter hand te stellen.

Artikel 7 RWE Gedragscode

De werknemer is verplicht alles te doen en na te laten wat een goed werknemer behoort te doen en na te laten. De werknemer zal zijn persoon en werkkracht naar beste vermogen inzetten om de belangen van de werkgever en de met deze verbonden ondernemingen te bevorderen. De werknemer is verplicht te handelen overeenkomstig de principes van de RWE gedragscode.

Artikel 8 Geschenken

Het is de werknemer verboden om in verband met de vervulling van zijn functie van derden, direct of indirect, enigerlei provisie, tegemoetkoming of vergoeding, in welke vorm ook, of geschenken aan te nemen of te bedingen. Het hiervoor gestelde geldt niet voorzover het gebruikelijke relatiegeschenken van geringe waarde (€ 50) betreft.

Artikel 9 Toepasselijk recht, CAO

9.1

Op deze overeenkomst is het Nederlandse recht van toepassing.

9.2

Op deze overeenkomst zijn van toepassing de CAO Productie- en Leveringsbedrijven (PLb), het bedrijfsprotocol en de concernregelingen, zoals deze luiden of zullen komen te luiden.

Aldus in tweevoud opgemaakt en getekend,

op te 's-Hertogenbosch
te.....

op

<<naam directeur>>

<<naam medewerker>>

Directeur Essent Service

Bijlage 3 Reglement Essent Controle op het ICT-gebruik

CONTROLE OP ICT-GEBRUIK

De verwerking van persoonsgegevens ten behoeve van de controle op ICT-gebruik geschiedt met inachtneming van de bepalingen van het Privacyreglement Essent N.V. november 2002 en van de in deze bijlage opgenomen aanvullende bepalingen.

1 Doel van de afspraken

1.1 Deze regeling geeft de wijze aan waarop in onze organisatie wordt omgegaan met gebruik van e-mail, internet en bedrijfsnetwerk, hierna ook te noemen "ICT Gebruik". Deze omvat gedragsregels ten aanzien van verantwoord gebruik en regels over de wijze waarop controle daarop plaatsvindt.

1.2 De faciliteiten die ter beschikking worden gesteld voor het verrichten van de werkzaamheden zijn primair bedoeld voor zakelijk gebruik. Beperkt privégebruik is toegestaan indien het de dagelijkse werkzaamheden niet stoort en geen additionele belasting geeft op het bedrijfsnetwerk.

1.3 In navolgende artikelen wordt bepaald op welke wijze het ICT Gebruik kan worden gecontroleerd en geregistreerd.

1.4. De controle op persoonsgegevens over ICT-gebruik vindt plaats met als doel:

- de interne controle op het gebruik van bedrijfsmiddelen en bedrijfsbeveiliging;
- controle op naleving van verboden gebruik van e-mail en internet;
- uitlekken van bedrijfsgeheimen tegengaan;
- voorkomen van negatieve publiciteit;
- tegengaan van (seksuele) intimidatie, agressie en geweld;
- begeleiding en individuele beoordeling;
- bewijs en archivering;
- systeem- en netwerkbeveiliging;
- kosten- en capaciteitsbeheersing.

2 Algemene uitgangspunten

2.1 De controle op e-mail en internetgebruik zal overeenkomstig dit reglement uitgevoerd worden. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de Wet Bescherming Persoonsgegevens (WBP) en in overleg met de Centrale Ondernemingsraad gehandeld worden.

2.2 Gestreefd wordt naar een goede balans tussen controle op verantwoord ICT Gebruik en bescherming van de privacy van werknemers op de werkplek.

2.3 Onverminderd hetgeen bepaald in artikel 8 van het reglement worden de Persoonsgegevens over ICT Gebruik niet langer bewaard dan strikt noodzakelijk voor een verantwoorde uitvoering van de bedrijfsdoelstelling.

2.4 De verantwoordelijke treft voorzieningen over de positie en integriteit van de netwerkbeheerder en/of afdeling netwerkbeheer en de controle daarop.

3 E-mail gebruik

3.1 Het versturen van e-mailberichten moet voldoen aan de volgende voorwaarden:

- een correcte vermelding van de afzender
- duidelijke onderwerpaanduiding (zowel bij zakelijke als voor persoonlijke mail)

3.2 Het is niet toegestaan om:

- dreigende, beledigende, seksueel getinte dan wel discriminerende berichten te versturen
- de goede naam van Essent in diskrediet te brengen
- ongeautoriseerd bedrijfsgeheimen door te geven
- kettingbrieven te versturen
- (bewust) virussen, trojans en/of cookies te versturen/ontvangen
- iemand elektronisch lastig te vallen
- anonieme berichten te versturen
- illegale aankopen te doen.

3.3. Ingeval van ontvangst van dreigende, beledigende, seksueel getinte, discriminerende e-mails, ontvangst van e-mails met virussen, trojans, cookies, kettingbrieven alsmede ingeval van ontvangst van andersoortige ongewenste en 'verboden' e-mails, dient onverwijld de netwerkbeheerder te worden geïnformeerd.

4 Internetgebruik

4.1 Het is niet toegestaan om:

- (bewust) sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten
- op internet in strijd met de wet of onethisch te handelen
- auteursrechten te schenden
- software en applicaties te downloaden
- online te gokken
- te chatten en gebruik te maken van Usenet (uitzonderingen zijn ter beoordeling van leidinggevende)

4.2 Het gebruik van Internet voor het transport van bestanden middels File Transfer Protocol(FTP) is aan specifieke regels onderhevig. Afhankelijk van de noodzaak en het bedrijfsrisico wordt FTP toegestaan, echter indien noodzakelijk kunnen additionele eisen voor beveiliging worden gesteld.

5 Controle

5.1 Controle op ICT Gebruik vindt slechts plaats in het kader van in artikel 2 onder 2 genoemde doelen. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle:

- voor het tegengaan van virussen en andere schadelijke programma's, in het kader van systeem- en netwerkbeveiliging, wordt het ICT Gebruik op geautomatiseerde wijze gecontroleerd.
- controle op het uitlekken van bedrijfsgeheimen vindt plaats op basis van steekproefsgewijze contentfiltering. Een verdacht bericht wordt apart gezet voor nader onderzoek.
- controle in het kader van het voorkomen van negatieve publiciteit vindt plaats op basis van contentfiltering. Verdachte berichten worden geautomatiseerd teruggestuurd naar de afzender en "verboden" sites geblokkeerd.
- controle in het kader van het tegengaan van seksuele intimidatie vindt op

geautomatiseerde wijze plaats. Verdachte berichten worden geautomatiseerd teruggestuurd naar de afzender.

- controle in het kader van het tegengaan van "verboden gebruik" vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.
- controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeersgegevens (tijd, hoeveelheid, omvang, etc.)

5.2 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een werknemer of een groep werknemers ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden alsmede gerichte controle van de opgeslagen gegevens. Ingeval van een dergelijke verdenking zal leidinggevende werknemer op de hoogte stellen van de uit te voeren gerichte controles tenzij dit naar de aard van het geval niet wenselijk is.

5.3 Controle van het gebruik van e-mail en internet beperkt zich in principe tot verkeersgegevens. Controle van het gebruik van het bedrijfsnetwerk beperkt zich in principe tot de omvang van de benodigde/gebruikte netwerkcapaciteit. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.

5.4 "Verboden" ICT Gebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.

5.5. De leidinggevende van de werknemers ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, alsmede eventueel de betrokken P&O functionaris, worden zo spoedig mogelijk door netwerkbeheerder op de hoogte gesteld. De leidinggevende zal beoordelen of gebruik gerechtvaardigd is en kan, indien gewenst passende maatregelen treffen conform de disciplinaire sancties zoals in toepasselijke CAO-bepalingen is vastgelegd.

5.6. E-mailberichten van medezeggenschapsleden, bedrijfsartsen en andere medewerkers met een vertrouwensfunctie zijn in beginsel uitgesloten van controle, met uitzondering van de controle op de veiligheid van het berichtenverkeer.

6 Beveiliging

6.1. Er kunnen passende beveiligingsmaatregelen worden getroffen om bedrijfsnetwerk te beschermen, zoals het gebruik van wachtwoorden voor toegang tot bedrijfsnetwerk en de instelling van automatische screen savers met wachtwoord. Beveiligingsmaatregelen zullen tijdig vooraf worden aangekondigd en worden gepubliceerd op intranet.

6.2 Op intranet zal praktische informatie worden gepubliceerd over de specifieke vormen van ICT gebruik alsmede over de werkwijze van netwerkbeheerder en de technische maatregelen die door netwerkbeheerder zijn getroffen om het bedrijfsnetwerk te optimaliseren alsmede te beveiligen.

Bijlage 4 Concernregeling Privacyreglement Essent

Concernregeling 18 Privacyreglement Essent N.V.

Toelichtingen:

- * Controle op ICT gebruik
- * Controle op mobiele telefoon

18.1 Algemene bepalingen

18.1.1 Begripsbepaling

In dit reglement wordt in aansluiting bij en in aanvulling op de Wet Bescherming Persoonsgegevens verstaan onder:

- a. de wet: de Wet Bescherming Persoonsgegevens;
- b. CBP: het College Bescherming Persoonsgegevens;
- c. het reglement: dit reglement (inclusief de bijlagen) van Essent welke van toepassing is op Essent NV alsmede de groepsmaatschappijen en dochtermaatschappijen van Essent NV met uitzondering van die groepsmaatschappijen en dochtermaatschappijen die een zelfstandige aanmelding onder de WBP hebben verricht en expliciet te kennen hebben gegeven niet onder dit reglement te vallen;
- d. persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
- e. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, 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;
- f. bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
- g. verantwoordelijke: Essent N.V. mede ten behoeve van de groepsmaatschappijen en dochtermaatschappijen van Essent NV met uitzondering van die groepsmaatschappijen en dochtermaatschappijen die een zelfstandige aanmelding onder de WBP hebben verricht,;
- h. bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
- i. personeel: personen in dienst van of werkzaam ten behoeve van de verantwoordelijke en haar groepsmaatschappijen en dochtermaatschappijen. Hieronder worden tevens begrepen ex-werknemers, gedetacheerden, tijdelijke inleenkrachten en sollicitanten;
- j. betrokkene: degene op wie een persoonsgegeven betrekking heeft;
- k. beheerder: degene die onder verantwoordelijkheid van de verantwoordelijke is belast met de dagelijkse zorg voor de verwerking van persoonsgegevens, voor de juistheid van de ingevoerde gegevens, alsmede voor het bewaren, verwijderen en verstrekken van gegevens;
- l. gebruiker: degene die onder verantwoordelijkheid van de beheerder bevoegd is persoonsgegevens in te voeren, te wijzigen en/of te verwijderen, dan wel van enigerlei uitvoer van de verwerking kennis te nemen;
- m. technische werkzaamheden: werkzaamheden die verband houden met onderhoud en reparatie van apparatuur en programmatuur;

- n. netwerkbeheerder: de afdeling(en) die de technische werkzaamheden uitvoeren;
- o. verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens;
- p. bijzondere persoonsgegevens: persoonsgegevens als bedoeld in artikel 16 van de wet.

18.1.2 Reikwijdte

Dit reglement is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens van personen in dienst van of werkzaam ten behoeve van Essent N.V. of haar groepsmaatschappijen en dochtermaatschappijen, ex-werknemers en sollicitanten, alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Dit reglement is voorts van toepassing op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

18.2 Doelbinding

18.2.1 Doelstellingen van de verwerking

De doelen dan wel de samenhangende doelen van de afzonderlijke en/of samenhangende verwerkingen voor de diverse categorieën van betrokkenen zijn door de verantwoordelijke, mede ten behoeve van haar groepsmaatschappijen en dochtermaatschappijen, met uitzondering van die groepsmaatschappijen en dochtermaatschappijen die een zelfstandige aanmelding onder de WBP hebben verricht, aangemeld.

18.2.2 Rechtmatige grondslag van de verwerking

De rechtmatige grondslag van de verwerking is gelegen in a) de uitvoering van de overeenkomst waarbij de betrokkene partij is, b) het gerechtvaardigde belang van de verantwoordelijke, c) een wettelijke verplichting van de verantwoordelijke, d) een vitaal belang van de betrokkene, dan wel - uitsluitend indien a), b), c) of d) niet van toepassing is - e) de ondubbelzinnige toestemming die de betrokkene heeft verleend.

18.2.3 Soorten van opgenomen persoonsgegevens en de wijze van verkrijging

- a. In de aanmelding voor de verwerking van de persoonsgegevens van het personeel is aangegeven welke soorten van persoonsgegevens ten hoogste worden verwerkt en op welke wijze deze gegevens worden verkregen.
- b. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf.
- c. Persoonsgegevens worden niet verzameld bij derden zonder de ondubbelzinnige toestemming van de betrokkene.
- d. Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
- e. Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de in de bijlagen genoemde doeleinden, toereikend, ter zake dienend en niet bovenmatig zijn.
- f. Bijzondere persoonsgegevens worden verwerkt met inachtneming van het bepaalde in de artikelen 16 tot en met 23 van de wet.
- g. De beheerder treft de nodige voorzieningen ter bevordering van de juistheid en volledigheid van de persoonsgegevens.

18.2.4 Verwijdering van opgenomen persoonsgegevens

- a. Persoonsgegevens die niet langer voor het doel noodzakelijk zijn, worden binnen 4 weken verwijderd.

- b. Na beëindiging van het dienstverband met, het verrichten van werkzaamheden ten behoeve van of de sollicitatieprocedure bij de verantwoordelijke of haar groepsmaatschappijen en dochtermaatschappijen, worden de gegevens niet langer bewaard dan strikt noodzakelijk is voor de verantwoorde uitoefening van de bedrijfsdoelstellingen, tenzij deze gegevens in verband met wettelijke verplichtingen langer bewaard moeten blijven.
- c. Verwijdering impliceert vernietiging of een zodanige bewerking dat het niet meer mogelijk is de persoon te identificeren.

18.3 Rechtstreekse toegang tot en verstrekking van Persoonsgegevens

18.3.1 Rechtstreekse toegang tot persoonsgegevens

- a. Uitsluitend de beheerder en de door de beheerder aangewezen gebruikers en bewerkers hebben, met het oog op de dagelijkse zorg voor het goed functioneren van de verwerking, rechtstreekse toegang tot persoonsgegevens.
- b. De personen, bedoeld in het eerste lid, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens, waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak tot mededeling voortvloeit.

18.3.2 Beheer en verstrekking van opgenomen persoonsgegevens

- a. Als beheerder van de verwerking treedt op de directeur HR Holding.
- b. Gegevens kunnen ten hoogste worden verstrekt aan de volgende personen of bedrijven/instellingen, voor zover noodzakelijk voor de onderscheiden doelen:
 - Binnen de organisatie:
 - a. de betrokkene;
 - b. de leidinggevende van betrokkene;
 - c. de beheerder;
 - d. de gebruikers;
 - e. de bewerkers;
 - f. de netwerkbeheerder(s);
 - g. de directie(s);
 - h. de financiële afdeling(en);
 - i. de juridische afdeling(en);
 - j. de verantwoordelijke;
 - Buiten de organisatie:
 - k. salarisadministratiekantoor;
 - l. Arbo-dienst, pensioenfondsen en uitvoeringsinstellingen;
 - m. vakbond, vakcentrale en personeelsvereniging;
 - n. externe adviseurs (o.a. financiële, juridische en (bedrijfs)organisatorische adviseurs), indien en voor zover voor hen reeds een geheimhoudingsplicht geldt.
 - sociale wetten.
- c. De verantwoordelijke informeert derden, die op vastgestelde wijze bepaalde persoonsgegevens verwerken, over de daaraan gestelde voorwaarden en beperkingen. De verantwoordelijke is aansprakelijk voor schade die de betrokkene lijdt door onrechtmatig gebruik door derden van door de verantwoordelijke rechtmatig aan die derden verstrekte persoonsgegevens.

18.3.3 Technische werkzaamheden en controle

- a. Personen die belast zijn met de uitvoering van technische werkzaamheden zijn gehouden tot geheimhouding van alle persoonsgegevens waarvan zij kennis (hebben) kunnen nemen. Zij zijn uitsluitend gerechtigd zich toegang te verschaffen tot persoonsgegevens en bestanden indien dit strikt noodzakelijk is voor de uitvoering van hun werkzaamheden.
- b. Voor de controle en toezicht op e-mail en internetgebruik alsmede gebruik van het bedrijfsnetwerk is een specifieke regeling opgenomen in bijlage 1. Voor de verwerking van en de controle op de gegevensverwerking in de call centra zal een specifieke regeling worden opgesteld die als bijlage 2 aan dit reglement zal worden toegevoegd.

18.3.4 Doorgifte van persoonsgegevens naar landen buiten de Europese Unie

De verantwoordelijke geeft geen persoonsgegevens door naar een bedrijf of vestiging in een land buiten de Europese Unie, dat geen passend beschermingsniveau heeft, tenzij voldaan is aan tenminste één van de volgende voorwaarden:

- a. met dat bedrijf of die vestiging is een contract gesloten overeenkomstig de door de Europese Commissie vastgestelde modelcontractbepalingen, welk contract voor wat betreft de verwerking van persoonsgegevens de instemming heeft van de Centrale Ondernemingsraad;
- b. de doorgifte is noodzakelijk in het kader van de arbeidsovereenkomst tussen de verantwoordelijke en de betrokkene;
- c. de betrokkene heeft een verklaring ondertekend, waarin hij de verantwoordelijke toestemming geeft voor de doorgifte. Die verklaring is in eenvoudige, begrijpelijke taal opgesteld, met specifieke informatie over het betrokken bedrijf of de betrokken vestiging, de door te geven persoonsgegevens, het doel van de doorgifte en de duur van de periode, waarin die verklaring wordt gebruikt.

18.4 Plichten van verantwoordelijke, beheerder en bewerker

18.4.1 Beveiliging

- a. De verantwoordelijke zal zorgdragen voor een passende technische en organisatorische maatregelen om verlies van gegevens of onrechtmatige verwerking tegen te gaan alsmede onnodige verzameling of verdere verwerking te voorkomen. Betreffende maatregelen zullen een passend beveiligingsniveau garanderen.
- b. De beheerder verwerkt overeenkomstig deze maatregelen.
- c. Indien gebruik wordt gemaakt van de diensten van een bewerker, legt de verantwoordelijke de wederzijdse verplichtingen met betrekking tot de omgang met persoonsgegevens schriftelijk in een overeenkomst met die bewerker vast. De bewerker verwerkt overeenkomstig diens overeengekomen verplichtingen.

18.4.2 Informatieplicht

- a. Indien de verantwoordelijke persoonsgegevens verkrijgt bij de betrokkene zelf, deelt hij de betrokkene vóór het moment van verkrijging zijn identiteit mee alsmede het doel van de verwerking waarvoor de gegevens zijn bestemd, tenzij de betrokkene hiervan reeds op de hoogte is.
- b. Indien de verantwoordelijke persoonsgegevens verkrijgt van een derde of door observatie van de betrokkene, deelt de verantwoordelijke de betrokkene op het

moment van vastlegging zijn identiteit mee alsmede het doel van de verwerking waarvoor de gegevens zijn bestemd.

- c. De verantwoordelijke verstrekt de in de leden 1 en 2 bedoelde informatie op een zodanige wijze dat de betrokkene er daadwerkelijk de beschikking over krijgt.

18.5 Rechten van de betrokkene

18.5.1 Recht van inzage, correctie en verzet

- a. Iedere betrokkene heeft recht op informatie, inzage en correctie (verbetering, aanvulling, verwijdering en/of afscherming) alsmede het recht van verzet, zoals geformuleerd in de artikelen 36 en 40 van de WBP .
- b. Het uitoefenen van die rechten kan in werktijd geschieden en dient middels een schriftelijk verzoek plaats te vinden bij de directe leidinggevende en/of de HR functionaris.
- c. Betrokkenen kunnen zich bij het uitoefenen van die rechten laten bijstaan.
- d. Aan het uitoefenen van die rechten zijn voor de betrokkene geen kosten verbonden.
- e. De beheerder draagt zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.
- f. De beheerder kan weigeren aan een verzoek te voldoen, indien en voor zover dit noodzakelijk is in verband met:
 - a. de opsporing en vervolging van strafbare feiten;
 - b. gewichtige belangen van anderen dan de verzoeker, de verantwoordelijke daaronder begrepen.
- g. De beheerder wijst betrokkenen op de mogelijkheden van rechtsbescherming en toezicht en op de rol daarvan van het College Bescherming Persoonsgegevens.

18.6 Rechtsbescherming en toezicht

18.6.1 Klachten en bemiddeling

Elke betrokkene kan een schriftelijke klacht indienen bij de directeur HR:

- a. tegen een beslissing op een verzoek als bedoeld in artikel 13 van dit reglement; en
- b. tegen de wijze waarop de verantwoordelijke, de beheerder, de gebruiker(s) of bewerker(s) de in dit reglement opgenomen regels uitvoert. Indien gewenst kan een externe deskundige worden ingeschakeld om bij het geschil te bemiddelen.

18.6.2 Toezicht op de naleving

Het College Bescherming Persoonsgegevens is op grond van de wet bevoegd toe te zien op de naleving van de in de wet opgenomen bepalingen alsmede op de naleving van de door Essent gedane melding bij het CBP.

18.7 Overige bepalingen

18.7.1 Scholing

De verantwoordelijke draagt zorg voor een regelmatige scholing van de beheerders en de gebruikers om te verzekeren dat ze de processen van persoonsgegevensverwerking, de daarvoor geldende regels en hun eigen rol daarin begrijpen.

18.7.2 Publicatie

Dit reglement wordt opgenomen in de map arbeidsvoorwaarden van Essent.

18.7.3 Wijzigingen en aanvullingen

Wijzigingen en aanvullingen van het reglement behoeven de instemming van de Centrale Ondernemingsraad.

Bijlage 5 Interview M. van Dijk

Gegevens geïnterviewde:

Naam: Mirjam van Dijk
Functie: Manager Industrial Relations
Organisatie: Essent
Datum: 5 maart 2015, 15:00

Welke rol heeft u bij de controle op internetgebruik door medewerkers van Essent?

‘Ik ben bij Essent verantwoordelijk voor de Concernregeling Privacyreglement, waar het ICT-reglement een bijlage bij is. Ik houd het toezicht dat Essent het Privacyreglement naleeft, en overleg hierover met de Centrale Ondernemingsraad van Essent. Daarnaast adviseer ik HR-adviseurs die te maken hebben met medewerkers die mogelijk het ICT-reglement overtreden. Ik kijk dan bijvoorbeeld hoe ernstig de overtreding is, en welke sanctie passend is.’

Welk internetgebruik vindt Essent acceptabel?

‘Veel medewerkers moeten natuurlijk voor hun werk het internet op. Zelf gebruik ik bijvoorbeeld regelmatig websites met juridische informatie en websites van de overheid. Een website die voor de ene medewerker zakelijk is, kan voor de ander privé zijn. Bijvoorbeeld een website voor een restaurant; deze bezoek je zakelijk als je een tafel reserveert voor een zakendiner, en privé als je een tafel boekt voor je gezin. We vinden het geen probleem als medewerkers af en toe privé websites bezoeken, maar het moet niet te verstoringend zijn voor het werk. Het is lastig om aan te geven waar de grens ligt. Een paar minuten per dag is normaalgesproken geen probleem; structureel een uur per dag wel. Daartussenin ligt een groot grijs gebied.’

Wordt er binnen Essent thuis gewerkt?

‘Binnen Essent hebben medewerkers de keus om op kantoor als thuis te werken. Dit moet natuurlijk wel de met de functie van de desbetreffende functie kunnen, dit geldt voorbal bij kantoorfuncties. Daarnaast is het niet de bedoeling dat medewerkers alle dagen thuis werken, maar twee á drie dagen is binnen Essent heel normaal. Daarbij geldt dat de medewerker thuis wel de mogelijkheid moet hebben om daar te werken, denk hierbij aan een aparte (rustige) ruimte. Er zijn ook medewerkers die helemaal niet thuiswerken, omdat ze zich daar bijvoorbeeld niet kunnen concentreren of merken dat ze niet productief genoeg zijn. Die medewerkers werken alle dagen op kantoor’

Hoe wordt momenteel bij Essent gecontroleerd op internetgebruik?

‘Bepaald internetgebruik wordt bij voorbaat tegengehouden; medewerkers kunnen vanaf hun werklaptop bijvoorbeeld geen gamingwebsites of adult entertainmentwebsites bezoeken. Verder vindt er geen generieke controle plaats; wel kan er een gerichte controle plaatsvinden als een leidinggevende ziet dat de medewerker zoveel internet dat het werk eronder lijdt. Er vindt dan echter eerst een gesprek plaats met de medewerker op basis van een vermoeden; we hebben nog nooit logs opgevraagd van internetgebruik in zo’n situatie. Voor de leidinggevende is het door Het Nieuwe Werken echter steeds

minder goed zichtbaar hoeveel een medewerker privé internet. Wanneer een of meerdere werknemers veel privé gebruik maken van het internet, dan kan dit op jaarbasis veel geld kosten. Essent bouwt momenteel nog steeds zijn personeelsbestand af, alle besparingen zijn welkom. Vandaar dat we nu graag willen weten wat we kunnen doen: wanneer mogen we controleren op overmatig internetgebruik?’

Wanneer ziet Essent het internetgebruik als privégebruik?

‘Binnen Essent is er geen vastgelegde definitie van het begrip privégebruik. Zoals het woord al zegt dient het te gaan om een ‘privé’ activiteit, dus wanneer het gebruik slechts voor de medewerker zelf van belang is, dan zien wij het als privégebruik.’

Ziet Essent een verschil tussen het gebruik van apparatuur van Essent (bijvoorbeeld laptop) en het gebruik van eigen apparatuur (BYOD / Bring Your Own Device)?

‘Voor Essent maakt het niet uit waar de medewerker op werkt. In beide gevallen vinden we het belangrijk dat de medewerker goed zijn werk kan doen, en in redelijkheid privé-dingen doet. Omdat het bij BYOD gaat om eigen apparatuur van de medewerker, waarop we toegang geven tot een deel van het Essent-netwerk, vinden we het wel belangrijk dat we extra vastleggen wat de medewerker mag doen, en wat wij als werkgever mogen. Dat is vastgelegd in een BYOD-gebruikersovereenkomst. Medewerkers ondertekenen deze bij de eerste BYOD-aanvraag. Later kunnen ze een tweede device toevoegen zonder opnieuw een gebruikersovereenkomst te tekenen.’

Welke apparatuur krijgen medewerkers met een kantoorfunctie die in dienst treden?

‘Medewerkers met een kantoorfunctie krijgen standaard een laptop en mobiele telefoon van Essent ter beschikking, zoals eerder gezegd mogen deze medewerkers er ook voor kiezen om hun eigen apparatuur te gebruiken voor zakelijke doeleinden.’

Welke overeenkomsten worden tussen Essent en zijn werknemers gesloten?

‘Essent sluit met zijn werknemers arbeidsovereenkomsten, in de vorm van arbeidscontracten voor bepaalde tijd of voor onbepaalde tijd.’

Bijlage 6 Interview P. Buijs

Gegevens geïnterviewde:

Naam: Pascal Buijs
Functie: Manager Risk Nederland
Organisatie: Essent
Datum: 27 maart 2015, 11:00

Welke rol heeft u bij de controle op internetgebruik door medewerkers van Essent?

‘Ik ben als Manager Risk verantwoordelijk voor het ICT-reglement van Essent en ben betrokken bij controles op onder andere fraude en internetgebruik.’

Welk internetgebruik vindt Essent acceptabel?

‘De meeste medewerkers moeten voor hun werkzaamheden gebruik kunnen maken van het internet. Dit internetgebruik is, zolang dit in het belang van Essent of klanten is, in de meeste gevallen toegestaan. Wanneer het echter om privégebruik gaat, dan is dit binnen redelijke grenzen tijdens werktijd toegestaan. In de pauzes is dit gebruik in ieder geval toegestaan, mits dit geen “verboden handelingen” zijn (zoals adult internetwebsites of het downloaden van films). Deze verboden handelingen zijn in de meeste gevallen door software afgeschermd.

Voor werknemers met een kantoorfunctie is niet altijd direct duidelijk wanneer er sprake is van pauze, dan dit het geval is bij een medewerker die volgens een rooster werkt.’

Wat is overmatig internetgebruik?

‘Hierover zijn in het ICT-reglement geen regels vastgelegd. Daarentegen staat in het ICT-reglement dat beperkt gebruik van faciliteiten, waaronder ook internet behoort, toegestaan is. Daarbij merk ik op dat dit de dagelijkse werkzaamheden niet mag verstoren en geen zware belasting (additionele belasting) voor het bedrijfsnetwerk van Essent mag opleveren. Er is van zware belasting bijvoorbeeld sprake bij het streamen van video’s of het beluisteren van radiozenders via het internet.’

Wanneer ziet Essent het internetgebruik als privégebruik?

‘Er is sprake van internetgebruik voor privégebruik wanneer dit gebruik op geen enkele wijze van belang is voor Essent. Denk hierbij aan het bestellen van kleding op Zalando of het gebruik maken van Facebook.’

Is het binnen Essent toegestaan om thuis te werken?

‘Bij Essent hebben de werknemers de keuze om thuis te werken. Werknemers loggen dan net zoals op kantoor in op het bedrijfsnetwerk van Essent. Ik maak hier zelf ook gebruik van.’

Hoe wordt er momenteel bij Essent gecontroleerd op internetgebruik?

‘Tot op heden heeft er binnen Essent nog geen controle op internetgebruik plaatsgevonden. In beginsel zal er een controle plaatsvinden, waaruit geen enkele individuele werknemer te herleiden is (dit noem ik ook wel de anonieme controle). Aan de hand van deze controle kan worden bekeken of er op het bedrijfsnetwerk van Essent “onregelmatigheden” plaatsvinden. Mocht aan de hand van bijvoorbeeld een anonieme tip een werknemer worden verdacht van overmatig internetgebruik, dan zullen eerst naar de gegevens uit de anonieme controle worden gekeken. Wanneer blijkt dat de betreffende werknemer de regels overtreedt, dan zal de verdachte werknemer in beginsel hierop worden aangesproken. In de meeste gevallen vindt er dan een gesprek tussen de leidinggevende en de werknemer plaats. Naderhand kan er nog een gerichte controle naar deze werknemer plaatsvinden.’

Wordt er binnen Essent conform het Privacyreglement en de daarbij behorende bijlage het ICT-reglement gehandeld?

‘Essent en zijn medewerkers dienen zich op grond van het Privacyreglement en het ICT-reglement aan de daarin genoemde regels te houden. Omdat er momenteel nog geen controles op internetgebruik hebben plaatsgevonden, is hier nog geen gebruik van gemaakt.’

Wat wordt er met de controle op verkeersgegevens verzameld en bij de controle op inhoud?

‘Bij een controle op verkeersgegevens wordt in de meeste gevallen het IP-adres, de internetprotocollen, de tijdsduur, de datum en de tijd verzameld. Wanneer er op inhoud wordt gecontroleerd, wordt er voornamelijk naar de bezochte internetwebsites, de afbeeldingen die de werknemer heeft bekeken of gedownload gekeken. Alleen al met het bijhouden van de verkeersgegevens kan het internetgedrag van de werknemers in kaart worden gebracht.’

Hoe worden de gegevens uit de controle op internetgebruik opgeslagen en (door wie) zijn deze bestanden naderhand raadpleegbaar?

‘Binnen het bedrijfsnetwerk van Essent bevinden zich een aantal servers, waarvan een aantal servers zorgen dat de werknemers van Essent toegang hebben tot het internet. Deze servers kunnen de handelingen van de werknemers op het internet registreren. De afdeling netwerkbeheer zorgt er voor dat bij een controle de juiste gegevens van de juiste werknemer(s) worden vastgelegd in een zogenaamd “logbestand”. Dit bestand kunnen de netwerkbeheerders van Essent naderhand raadplegen. Aan de hand van de gegevens die in dit bestand staan kan bijvoorbeeld worden beoordeeld of de werknemer overmatig van het internet gebruik maakt of bepaalde “verboden” internetwebsites heeft bezocht.’

Welke beveiligingsmaatregelen treft Essent met betrekking tot de persoonsgegevens?

‘Essent treft verschillende maatregelen om de persoonsgegevens van onze werknemers zo goed mogelijk te beveiligen. Het Privacyreglement wijst de werknemers aan die toegang hebben tot de persoonsgegevens en aan welke personen binnen en buiten Essent de persoonsgegevens verstrekt mogen worden. Tevens worden servers en gebouwen waar de servers staan beveiligd door een beveiligingsbedrijf, camerasystemen en toegangspasjes. De ruimte waar de servers staan zijn alleen toegankelijk voor

netwerkbeheerders of andere personen die hier (in geval van nood) toegang tot moeten kunnen hebben. Deze toegang is eveneens alleen mogelijk met een pasje. Verder zijn de servers beveiligd door middel van de standaardsoftware, extra beveiligingssoftware en worden de persoonsgegevens encrypt op de server. De afdeling netwerkbeheer zorgt dat alle software up-to-date blijft. Wanneer zij het nodig achten dat er nieuwe software dient te worden aangeschaft zullen zij hiervan melding maken.'

Zijn er extra beveiligingsmaatregelen genomen met betrekking tot de netwerkbeheerders van Essent?

'Netwerkbeheerders worden, evenals al het andere personeel met een functie waar dit nodig wordt geacht, gecontroleerd op de integriteit.'

Wat zijn de verschillen tussen het gebruik van BYOD en gebruik van Essent apparatuur/middelen met betrekking tot de toegang tot het bedrijfsnetwerk?

'Bij het gebruik van BYOD heeft de werknemer dezelfde toegang op het bedrijfsnetwerk van Essent als bij het gebruik van apparatuur van Essent. Het enige verschil tussen BYOD en apparatuur van Essent is dat de apparatuur in het geval van BYOD in eigendom van de werknemer is en dat onder bepaalde omstandigheden er extra beveiligingssoftware op de BYOD-apparatuur kan worden (dit is overeenkomstig de BYOD-gebruikersovereenkomst). Werknemers kunnen dus niet kiezen uit het bedrijfsnetwerk, dit is voor iedere werknemer hetzelfde.'

Bijlage 7 Nieuw ICT-reglement

In deze bijlage is het oude ICT-reglement naar aanleiding van het onderzoek aangepast. In paragraaf 5.3 van dit rapport zijn de belangrijkste wijzigingen in dit nieuwe ICT-reglement aangegeven.

ICT- en internetreglement

Reglement treedt in werking op: dd-mm-jj

Reglement is binnen Essent gepubliceerd op: dd-mm-jj

Algemene toelichting

Het ICT- en internetreglement (hierna: reglement), is een bijlage van de Concernregeling nr. 18 (het Privacyreglement Essent N.V.) en reglementeert het gebruik van internet, e-mail en het bedrijfsnetwerk binnen Essent (hierna: ICT-gebruik). Het doel van dit reglement is het voeren van een eenduidig beleid omtrent het ICT-gebruik.

Artikel 1 Reikwijdte

Het reglement is van toepassing op alle werknemers van Essent (hierna: werknemers).

Artikel 2 Gebruik van internet, e-mail en bedrijfsnetwerk

Werknemers dienen verantwoord met het ICT-gebruik om te gaan. Het ICT-gebruik dat ter beschikking is gesteld voor het verrichten van werkzaamheden, is primair bedoeld voor zakelijk gebruik. Privégebruik met betrekking tot ICT-gebruik is alleen voor werknemers toegestaan, mits dit gebruik in overeenstemming is met dit reglement en geen additionele belasting geeft op het bedrijfsnetwerk.

Artikel 3 Aanvullende regels E-mailgebruik

1. Het versturen van e-mailberichten moet voldoen aan de volgende voorwaarden:

- a) een correcte vermelding van de afzender; en
- b) een duidelijke onderwerpaanduiding (zowel bij zakelijke als voor persoonlijke mail).

2. Het is niet toegestaan om:

- a) dreigende, beledigende, seksueel getinte dan wel discriminerende berichten te versturen;
- b) de goede naam van Essent in diskrediet te brengen;
- c) ongeautoriseerd bedrijfsgeheimen door te geven;
- d) kettingbrieven te versturen;
- e) (bewust) virussen, trojans en/of cookies te versturen/ontvangen;
- f) iemand elektronisch lastig te vallen;
- g) anonieme berichten te versturen;
- h) illegale aankopen te doen.

3. Ingeval van ontvangst van dreigende, beledigende, seksueel getinte, discriminerende e-mails, ontvangst van e-mails met virussen, trojans, cookies, kettingbrieven alsmede ingeval van ontvangst van andersoortige ongewenste en 'verboden' e-mails, dient onverwijld de netwerkbeheerder te worden geïnformeerd.

Artikel 4 Toezicht en controle

1. De controle op ICT-gebruik geschiedt met inachtneming van de bepalingen uit de Concernregeling nr. 18 en de in deze bijlage opgenomen aanvullende bepalingen, alsmede met inachtneming van de relevante wettelijke bepalingen.

Artikel 5

1. In de navolgende artikelen wordt bepaald op welke wijze het ICT-gebruik binnen Essent kan worden gecontroleerd en geregistreerd.

2. De controle op persoonsgegevens met betrekking tot ICT-gebruik vindt op grond van minimaal één van de onderstaande doelen plaats:

- a) de interne controle op het gebruik van bedrijfsmiddelen en bedrijfsbeveiliging;
- b) de controle op naleving van 'verboden gebruik' van e-mail en internet;
- c) de bescherming van bedrijfsinformatie, ongeacht de classificatie;
- d) het voorkomen van negatieve publiciteit;
- e) het tegengaan van (seksuele) intimidatie, agressie en geweld;
- f) begeleiding en individuele beoordeling;
- g) bewijs en archivering;
- h) systeem- en netwerkbeveiliging;
- i) kosten- en capaciteitsbeheersing.

3. Gestreefd wordt naar een goede balans tussen controle op verantwoord ICT-gebruik en bescherming van de privacy van werknemers op de werkplek.

Artikel 6 Verboden internetgebruik

1. Het is niet toegestaan om:

- a) (bewust) sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- b) op internet in strijd met de wet of onethisch te handelen;
- c) auteursrechten te schenden;
- d) software en applicaties te downloaden;
- e) online te gokken;
- f) te chatten en gebruik te maken van Usenet (uitzonderingen zijn ter
- g) beoordeling van leidinggevende);
- h) overmatig gebruik te maken van het internet voor privédoeleinden.

2. Er is sprake van overmatig internetgebruik voor privédoeleinden, wanneer aan dit gebruik buitenproportioneel veel tijd wordt besteed, geen geval storend is voor, dan wel ten kosten gaat van, het uitvoeren van de werkzaamheden

3. Het gebruik van internet voor het transport van bestanden middels File Transfer Protocol (hierna: FTP) is aan specifieke regels onderhevig. Afhankelijk van de noodzaak en het bedrijfsrisico wordt FTP toegestaan, echter indien noodzakelijk kunnen additionele eisen voor beveiliging worden gesteld.

Artikel 7 Controle op ICT-gebruik

1. Controle op ICT-gebruik vindt slechts plaats in het kader van de in artikel 5 lid 2 van dit reglement genoemde doelen. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle.

2. Controle op ICT-gebruik vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien één werknemer of meerdere werknemers ervan wordt of worden verdacht de regels in dit reglement te overtreden, kan gedurende een van tevoren vastgestelde periode gerichte controle plaatsvinden alsmede gerichte controle van de opgeslagen gegevens. Deze controle vindt in beginsel zo kort mogelijk plaats.

Ingeval van een gerichte controle zal de leidinggevende de werknemer voorafgaand aan de gerichte controle op de hoogte stellen van zijn identiteit en het doel van de controle, tenzij er sprake is van een zwaarwegend belang en een redelijke verdenking van strafbare of verboden handelingen die door de werknemer(s) worden verricht.

3 'Verboden', niet toegestaan, overmatig of ongewenst ICT-gebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Ingeval van controle geldt hetgeen uit lid 2 van dit artikel.

4. Controle op het gebruik van e-mail en internet beperkt zich in beginsel tot verkeersgegevens. Controle op het gebruik van het bedrijfsnetwerk beperkt zich in principe tot de omvang van de benodigde/gebruikte netwerkcapaciteit. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.

5. E-mailberichten van medezeggenschapsleden, bedrijfsartsen en andere medewerkers met een vertrouwensfunctie zijn in beginsel uitgesloten van controle, met uitzondering van de controle op de veiligheid van het berichtenverkeer.

Artikel 8 Sancties

1. De leidinggevende van de werknemers ten aanzien van wie geconstateerd is dat zij zich niet aan dit reglement houden, alsmede eventueel de betrokken HR functionaris, worden hierover zo spoedig mogelijk door netwerkbeheerder op de hoogte gesteld. De leidinggevende zal beoordelen of het gebruik gerechtvaardigd is en kan, indien gewenst passende maatregelen treffen conform de disciplinaire sancties die in toepasselijke CAO-bepalingen zijn vastgelegd.

Artikel 9 Bewaartermijn persoonsgegevens

1. De persoonsgegevens met betrekking tot het ICT-gebruik worden niet langer bewaard dan strikt noodzakelijk is voor een verantwoorde uitvoering van de doelstelling uit artikel 5 lid 2 in dit reglement.

Artikel 10 Rechten van de werknemers

Werknemers kunnen gebruik maken van de rechten die hen overeenkomstig het artikel 18.5.1 Privacyreglement Essent N.V. toekomen.

Artikel 11 Positie en integriteit netwerkbeheer

1. De verantwoordelijke treft voorzieningen over de positie en integriteit van de netwerkbeheerder en/of afdeling netwerkbeheer en de controle daarop.

Artikel 12 Beveiliging

1. Er kunnen passende beveiligingsmaatregelen worden getroffen om het bedrijfsnetwerk te beschermen, zoals het gebruik van wachtwoorden voor toegang tot het bedrijfsnetwerk en het instellen van automatische screensavers met wachtwoord. Beveiligingsmaatregelen zullen tijdig vooraf worden aangekondigd en worden gepubliceerd op het intranet.

2. Op intranet zal praktische informatie worden gepubliceerd over de specifieke vormen van ICT-gebruik alsmede over de werkwijze van netwerkbeheerder en de technische maatregelen die door netwerkbeheerder zijn getroffen om het bedrijfsnetwerk te optimaliseren alsmede te beveiligen.

Artikel 13 Slotbepaling

Indien zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de Wet bescherming persoonsgegevens (Wbp) en in overleg met de Centrale Ondernemingsraad (COR) worden gehandeld.