



Lengkeek, Laarman & De Hosson

EXPERTS • TAXATEURS • ADVISEURS

Lengkeek,
Laarman
& De
Hosson

10 januari

2012

In hoeverre voldoet de verwerking en opslag van persoonsgegevens door Lengkeek, Laarman & De Hosson aan de eisen die de Wet bescherming persoonsgegevens hieraan stelt?

Privacy
Compliance

Auteur:	Wouter Nieuwesteeg
Studentnummers:	2017482/164153
Opleiding:	Juridische Hogeschool (Tilburg)
Datum:	10 januari 2012, Tilburg
Opdrachtgever:	Lengkeek, Laarman & De Hosson
Afstudeermentor:	Mevr. M. Verhappen
Afstudeerdocent:	Mevr. Mr. Drs. A.M.M. van Breugel
Afstudeerperiode:	September 2011/Januari 2012



Lengkeek, Laarman & De Hosson
EXPERTS • TAXATEURS • ADVISEURS

‘Lengkeek, Laarman en De Hosson, Privacy Compliance’

In hoeverre voldoet de verwerking en opslag van persoonsgegevens door Lengkeek, Laarman en De Hosson aan de eisen die de Wet bescherming persoonsgegevens hieraan stelt?

Auteur:	Wouter Nieuwesteeg
Studentnummers:	2017482/164153
Opleiding:	Juridische Hogeschool (Tilburg)
Datum:	10 januari 2012, Tilburg
Opdrachtgever:	Lengkeek, Laarman & De Hosson
Afstudeermentor:	Mevr. M. Verhappen
Afstudeerdocent:	Mevr. Mr. Drs. A.M.M. van Breugel
Afstudeerperiode:	September 2011/Januari 2012

Voorwoord

Gedurende de periode september 2011 tot januari 2012 heb ik aan dit afstudeeronderzoek gewerkt op de Eindhovense vestiging van Lengkeek.

Via deze weg wil ik mijn dank uitspreken aan verschillende personen. Allereerst aan mijn begeleider binnen Lengkeek, Margret Verhappen. Haar prettige manier van optreden en uitstekende ondersteuning leverden niet alleen een belangrijke bijdrage aan mijn onderzoek, maar hebben deze periode voor mij ook tot een prettige ervaring gemaakt.

Financieel directeur Klaas Mijnheer nam tweemaal uitgebreid de tijd om met mij van gedachten te wisselen. Hem wil ik hiervoor ook van harte bedanken.

Daarnaast wil ik Sandra van Breugel bedanken voor de heldere en prettige begeleiding vanuit de Juridische Hogeschool. Haar directe benadering van de problematiek heb ik zeer weten te waarderen.

Uiteraard wil ik ook graag alle collega's bij Lengkeek bedanken voor hun openhartige medewerking aan het onderzoek. Ik heb me altijd zeer welkom gevoeld binnen Lengkeek. Verder wil ik Lengkeek nog bedanken voor het beschikbaar stellen van alle noodzakelijke middelen waarvan ik in de afgelopen maanden ruimhartig gebruik heb mogen maken.

Tot slot hoop ik dat de lezer net zoveel plezier heeft met het lezen van dit rapport als ik heb gehad met het maken ervan.

Eindhoven 8 januari 2012,

.....

Wouter Nieuwesteeg

Inhoudsopgave

Samenvatting.....	
Afkortingen.....	
1 - Inleiding.....	1
1.1 Organisatie	1
1.2 Privacy	1
1.3 OR problematiek.....	2
1.4 ISO 9001/2008 certificatie.....	2
1.5 Wet Harrewijn	2
1.6 Vraagstelling	2
1.7 Aanpak.....	3
2 - De Wbp & persoonsgegevens	5
2.1 Geschiedenis.....	5
2.2 EU-privacyrichtlijn	6
2.3 Terminologie uit de Wbp.....	7
2.4 Betrokkene	8
2.5 De verantwoordelijke	8
2.6 De bewerker	9
2.7 Reglement en gedragscode	10
3 – De gegevensverwerking binnen Lengkeek	12
3.1 Fysieke werknemersgegevens.....	12
3.2 Lengkeek Automatiserings Systeem (LAS).....	13
3.3 Fysieke klantgegevens (dossiers)	13
3.4 Werknemersgegevens buiten ADP	13
4 – Gegevensopslag en beveiliging.....	17
4.1 Fysieke opslag.....	18
4.2 Digitale opslag	18
4.3 Beveiliging in de wet.....	19
4.4 Beoordeling van beveiliging via risicoklassen.....	20
5 – Lengkeeks rechten en plichten.....	24

5.1 Meldingsplicht CBP	24
5.2 Melding aan medewerkers.....	25
5.3 Inzagerecht	26
5.4 Recht op correctie	26
5.5 Recht op Verzet	26
5.6 Bewaartermijn	27
5.7 Rol van de OR	28
6 – De Wet Harrewijn en de maatschap Lengkeek	30
6.1 Artikel 2:396 BW	31
6.2 Artikel 2:397 BW.....	31
6.3 Privacy & de Wet Harrewijn	31
7 – Conclusies en aanbevelingen.....	33
Literatuurlijst	36
Evaluatie	38

Samenvatting

Hoofdstuk 1 geeft een inleiding in het bedrijf Lengkeek, Laarman & De Hosson (Lengkeek) en zet het onderzoek uiteen. Lengkeek is een bedrijf dat zich specialiseert in expertises, taxaties en bouwkundige opnames. Mede door vragen vanuit de OR, in combinatie met opmerkingen van de ISO auditor, is besloten dit onderzoek naar de privacy compliance te laten uitvoeren.

In dit onderzoek wordt bekeken in hoeverre de verwerking en opslag van persoonsgegevens door Lengkeek voldoet aan de eisen die de wet hieraan stelt. De kern van het onderzoek bestaat uit punten die door de OR en het bestuur zijn aangedragen. In brede zin is het ook een rapport dat als handleiding voor eventuele toekomstige vraagstukken kan dienen.

In hoofdstuk 2 worden de wet en enkele belangrijke termen behandeld. Deze termen worden ook toegepast op Lengkeeks huidige situatie. Ook wordt bekeken of er nog nadere regelgeving bestaat in het interne reglement, de algemene gedragscode of vanuit de brancheorganisatie.

Hoofdstuk 3 behandelt de gegevensverwerking binnen Lengkeek. Alle fysieke en digitale systemen waarin persoonsgegevens worden verwerkt worden beschreven. Ook wordt bekeken wat het doel van die verwerkingen is en of er een juiste grondslag voor bestaat.

Hoofdstuk 4 bespreekt hoe de in het vorige hoofdstuk benoemde gegevens worden beveiligd. Ook wordt besproken in welke mate deze beveiliging voldoet in Lengkeeks specifieke situatie.

Hoofdstuk 5 behandelt verschillende rechten en plichten van Lengkeek zoals de meldingsplicht en de informatieplicht. Ook worden enkele rechten van de betrokkene behandeld en wordt de rol van de OR op privacygebied bekeken.

Hoofdstuk 6 is een min of meer op zichzelf staand hoofdstuk dat een apart vraagstuk behandelt dat binnen de organisatie speelde. Hierin wordt bekeken of de Wet Harrewijn wel of niet op Lengkeek van toepassing is.

Tenslotte worden in hoofdstuk 7 de conclusies en aanbevelingen uit dit onderzoek nog eens apart opgesomd.

Afkortingen

ADP	Automatic Data Processing
Art.	Artikel
BV	Besloten Vennootschap
BW	Burgerlijk Wetboek
CBP	College Bescherming Persoonsgegevens
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
ICT	Informatie- en Communicatietechnologie
ISO	International Organization for Standardization
IVBPR	Internationaal Verdrag inzake Burgerrechten en Politieke Rechten
KvK	Kamer van Koophandel
LAS	Lengkeek Automatiserings Systeem
NIVRE	Nederlands Instituut Van Register Experts
OQM	Tag Online Quality Manager
OR	Ondernemingsraad
UVRM	Universele Verklaring van de Rechten van de Mens
VN	Verenigde Naties
VPN	Virtual Private Network
Wbp	Wet Bescherming Persoonsgegevens
WOR	Wet op de Ondernemingsraden
WPR	Wet Persoonsregistratie

1 - Inleiding

Lengkeek, Laarman & De Hosson (Lengkeek) is een bedrijf dat zich specialiseert in expertises, taxaties en bouwkundige opnames en dat door samenvoegingen met andere taxatiebureaus en expertisebureaus is uitgegroeid tot een top drie speler op de Nederlandse markt. Vanuit full service kantoren in Rotterdam, Amsterdam, Zwolle, Eindhoven en Maastricht bedient Lengkeek de gehele Nederlandse markt.

1.1 Organisatie

Onder de naam Lengkeek Expertises worden praktisch alle vormen van schade-expertises verricht. Met name de deskundigheid op het gebied van brand en varia is groot. Denk hierbij aan constructieschade, aansprakelijkheid, technische schade, regres en deskundigenonderzoek. Bij complexe schades wordt meestal in teams gewerkt, waarbij iedere schade-expert zijn eigen inbreng heeft. In geval van calamiteiten zijn door de grootte van de organisatie altijd alle gevraagde schade-experts te leveren. Lengkeek Expertises werkt voornamelijk voor verzekeraars, maar ook voor verzekerden, bedrijven en instellingen die deskundige bijstand zoeken.

Lengkeek Taxaties verzorgt alle denkbare vormen van taxaties voor verzekerings- en bedrijfseconomische doeleinden. Lengkeek Taxaties werkt zowel voor ondernemingen als particulieren en verzorgt objectieve waardebeoordelingen voor elk gewenst doel. Er wordt gewerkt met gecertificeerde taxateurs die, afhankelijk van hun expertise, bij een van de drie brancheorganisaties zijn ingeschreven.

De grote bebouwingsdichtheid in Nederland maakt een bouwkundige opname vrijwel altijd noodzakelijk. Heiwerkzaamheden geven trillingen door aan de ondergrond, waardoor een naburige eigenaar schade kan ondervinden van de bouwwerkzaamheden. Bij graafwerkzaamheden en het onttrekken van grondwater is het eveneens verstandig om een vooropname te laten uitvoeren. Zodoende beschermt men zich ook tegen onterechte schadeclaims. Bij gebrek aan bewijs krijgt de gedupeerde namelijk veelal het voordeel van de twijfel.

Lengkeek Bouwkundige Opnames beschikt over een team van deskundigen die opnames verzorgen waarmee men voorbereid is op schadeclaims van gedupeerden. Ook worden adviezen verstrekt en metingen verricht. Bij eventuele claims verricht Lengkeek als het nodig is een na-opname. De collega's van Lengkeek Expertises kunnen eventueel de volledige schadeafhandeling uitvoeren.

1.2 Privacy

In het werkgebied van Lengkeek spelen vertrouwen, integriteit en professionaliteit een grote rol. Hierbij sluit het onderwerp privacy goed aan. Klanten van Lengkeek dienen er blind op te kunnen vertrouwen dat met hun, soms gevoelige, gegevens correct wordt omgegaan. Mocht naar buiten komen dat hierin wordt tekortgeschoten dan heeft dit voor Lengkeek mogelijk nadelige gevolgen. De binnenkomst van opdrachten is namelijk niet zelden een kwestie van vertrouwen en gunnen.

Lengkeek werkt altijd in het belang van één partij, voornamelijk verzekeraars. Lengkeek beoordeelt vaak of de verzekeraar op de juiste gronden wordt aangesproken. In dit proces van beoordeling komt informatie naar voren. In het geval van een aansprakelijkheidsverzekering bijvoorbeeld, zal vaak sprake zijn van verklaringen van verschillende personen. Wanneer de inhoud van deze verklaringen niet goed afgeschermd is kan dit zowel economische als juridische gevolgen hebben.

Vanuit de verzekeringsovereenkomst is de verzekerde verplicht alle informatie te verstrekken die de expert nodig heeft voor de vaststelling van de schade en het beoordelen van het risico (de verzekerde zaak). Een dergelijke verplichting weegt zwaar. De verzekerde moet er dan ook blind op kunnen vertrouwen dat, wanneer hij deze informatie verstrekt, deze ook met zorg wordt behandeld.

In de kern van de zaak komt het er op neer dat de onderzoeken die Lengkeek uitvoert geen openbare onderzoeken zijn. Een simpel voorbeeld is jaarrekeningen. Wanneer Lengkeek een jaarrekening nodig heeft om een zaak te beoordelen, wordt niet de openbare KvK jaarrekening gebruikt maar die van de accountant, een veel gedetailleerdere vorm van informatie waarbij men in theorie ieder bonnetje kan zien dat de directeur heeft gedeclareerd. Ook is het zo dat wanneer bedrijf A een vordering heeft op bedrijf B en de jaarrekeningen van bedrijf B zijn onderhanden bij Lengkeek, het consequenties kan hebben wanneer deze informatie ongewild bij bedrijf A terecht komt. Op een nog persoonlijker niveau worden vaak strafrechtelijke gegevens verwerkt in het kader van een onderzoek.

Privacy is dus voor een bedrijf als Lengkeek van groter belang dan voor veel andere bedrijven omdat de informatie gevoelig is en de branche grotendeels drijft op onderling vertrouwen.

1.3 OR problematiek

Lengkeeks OR ontving in 2010 een verzoek om een advies conform art. 25 WOR, betreffende het toegangscontrolesysteem voor werknemers dat in Rotterdam in gebruik was genomen. Het was niet duidelijk wat het systeem precies kon registreren en wie inzicht had in de gegevens. Aan de hand van die vraag kwam de OR er achter dat nooit eerder met het bestuur is afgestemd hoe Lengkeek met verschillende persoonsgegevens omgaat. In dat kader heeft de OR een aantal vragen opgesteld betreffende de interne privacy (die van het personeel) en deze per brief aan het bestuur van Lengkeek toegezonden.

1.4 ISO 9001/2008 certificatie

Lengkeek beschikt al jaren over een zogenaamd ISO 9001:2008 certificaat. Iedere drie jaar toetst een onafhankelijke auditor de interne en externe processen van de organisatie aan de normen van het ISO. Tijdens de laatste audit in 2010 maakte de auditor opmerkingen betreffende de externe privacy van Lengkeek. Het gaat dan dus om gegevens van klanten/opdrachtgevers. Zo liggen er bijvoorbeeld losse dossiers op bureaus en in open kasten. De opmerkingen van de auditor zijn mondeling gemaakt en dus niet terug te vinden in het auditrapport. Al voor dat de auditor zijn kritiek gaf lag er de vraag vanuit de OR aan de directie betreffende de interne privacy. Zodoende is besloten de vragen over interne en externe privacy te behandelen in dit onderzoek.

1.5 Wet Harrewijn

De Wet Harrewijn is een recente toevoeging aan de WOR die het informatierecht van de OR uitbreidt. Omdat de OR zich wil beroepen op dit recht, speelt nu de vraag of deze wet eigenlijk wel op Lengkeek van toepassing is. In een reactie aan de OR heeft de directie al aangegeven van mening te zijn dat dit niet zo is. Ook op deze vraag dient het rapport zo goed mogelijk duidelijkheid te scheppen.

1.6 Vraagstelling

Privacy blijft echter het hoofdonderwerp van het rapport. Privacy is een ruim begrip en behelst niet alleen de bescherming van persoonsgegevens maar ook de eerbiediging van de persoonlijke levenssfeer in het algemeen. Verschillende regels zijn relevant voor de bescherming van privacy. Op het verwerken van persoonsgegevens is vooral de Wbp van belang, terwijl voor de verdere bescherming van de persoonlijke levenssfeer juist art. 8

EVRM, de Grondwet, het onrechtmatige daadsrecht en bijzondere wetten zoals de auteurswet van belang zijn.¹ In dit onderzoek is gekozen om de Wbp als uitgangspunt te nemen, omdat deze wet in de praktijk voor grote organisaties het meest van belang is. De hoofdvraag luidt:

- *In hoeverre voldoet de verwerking en opslag van persoonsgegevens door Lengkeek, Laarman & De Hosson aan de eisen die de Wbp hieraan stelt?*

Deelvragen

- *Wat zijn persoonsgegevens?*
- *Welke persoonsgegevens verwerkt Lengkeek?*
- *Welke persoonsgegevens vallen onder de Wbp?*
- *Welke persoonsgegevens slaat Lengkeek op?*
- *Met welk doel verwerkt Lengkeek deze gegevens?*
- *Wie verwerkt deze gegevens?*
- *Hoe worden deze gegevens opgeslagen?*
- *Hoe worden de opgeslagen gegevens beveiligd?*
- *Wie heeft toegang tot de opgeslagen gegevens?*
- *Welke rechten en plichten heeft Lengkeek met betrekking tot de door haar verwerkte persoonsgegevens?*
- *Hoe verhouden zich privacyaspecten tot een ISO certificering?*
- *In hoeverre zijn de artikelen 31d & e van de WOR van toepassing op de maatschap Lengkeek en welke privacy problematiek brengt dit met zich mee?*²

1.7 Aanpak

In dit onderzoek zal gekeken worden welk soort gegevens door Lengkeek worden verwerkt. Twee belangrijke digitale systemen voor gegevensverwerking binnen de organisatie zijn ADP en LAS. ADP is een systeem, beheerd door een gelijknamig bedrijf dat de personeelsregistratie van Lengkeek verzorgt. Lengkeek kan zelf alle gegevens die in het ADP-systeem zijn opgenomen bekijken en muteren. ADP is marktleider in dergelijke systemen, in het onderzoek wordt er vanuit gegaan dat ADP rechtmatig met persoonsgegevens omgaat. In ADP's 'verklaring van informatiebeveiliging' verklaart zij ook dat de kwaliteit van haar beveiliging tenminste voldoet aan alle relevante in de Nederlandse wet gestelde eisen voor informatiebeveiliging, met name die uit de Wbp en de EU-richtlijn. Ook de door ADP geleverde software die door Lengkeek wordt gebruikt zou voldoen aan dezelfde eisen.

De externe personeelsregistratie valt derhalve buiten dit onderzoek. Wel wordt kort ingegaan op de juridische verhouding tussen ADP en Lengkeek op privacygebied. Hetzelfde geldt voor de diensten van Iron Mountain gegevensopslag waarvan Lengkeek gebruik maakt.

LAS is een intern systeem waarin gegevens en dossiers van klanten en opdrachtgevers digitaal worden opgeslagen. Het LAS systeem zal wel behandeld worden in dit onderzoek.

Voor ieder digitaal bestand is ook een fysiek bestand aanwezig waar naar gekeken moet worden. Sommige gegevens die in ADP staan zijn ook in fysieke vorm aanwezig binnen Lengkeek. Hier wordt wel aandacht aan besteed. Op de openbare site, Lengkeeks intranet, het kwaliteitsmanagementsysteem OQM en de "Openbare Mappen" van het e-mailsysteem Outlook staan tevens persoonsgegevens van werknemers. Daarnaast zijn er ook nog andere werknemersgegevens die buiten ADP vallen zoals gegevens over tankgedrag, belgedrag, deurregistratie, e-mailverkeer, computergebruik, parkeergedrag en cameratoezicht. Tot slot

¹ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 13.

² Een belangrijke vraag die op verzoek van de organisatie wordt meegenomen in dit onderzoek en die deels buiten de hoofdvraag valt.

zijn er nog de gegevens die doorgespeeld worden naar de Arbodienst, Centraal Beheer Achmea (werknemersverzekeringen) en Nationale Nederlanden (pensioenen) die hun eigen privacyprotocol zullen hebben. Om tijdstechische redenen worden deze laatste drie buiten beschouwing gelaten.

Omdat de Wbp een kaderwet is die van toepassing is op allerlei vormen van persoonsgegevensverwerking is het extra belangrijk dat de gegevens vanuit de organisatie correct zijn. De algemene materiële normen van de wet zullen op ondernemingsniveau nader ingevuld worden aan de hand van de specifieke situaties binnen Lengkeek.³ Vanuit juridisch oogpunt is het ook niet nodig dat constant onderscheid wordt gemaakt tussen interne en externe privacy. Dezelfde regels zijn immers op beide vormen van toepassing. Toch zal dit onderscheid soms worden gemaakt ter verduidelijking voor de lezer.

Zoals gezegd is de Wbp de leidraad van dit onderzoek. Er zal echter ook gekeken worden of het ISO en brancheorganisatie NIVRE eigen privacyrichtlijnen hebben en zo ja, hoe deze zich verhouden tot de Wbp en Lengkeeks feitelijke situatie.

Er is in dit onderzoek zo veel mogelijk gebruik gemaakt van de primaire bron: de wet en regelgeving, die ook aangewend wordt om standpunten te bevestigen. Ook bij het interviewen is belangrijke verkregen informatie aan andere betrokkenen voorgelegd om deze informatie te controleren (second opinion).

Bij bronvermelding en voetnoten is de '*Leidraad voor juridische auteurs*' gehanteerd.

Voor het onderzoek is gebruik gemaakt van de volgende bronnen:

- Wet- en regelgeving.
- Literatuur.
- Stukken en studies van het CBP.
- Jurisprudentie.
- Interne stukken (jaarrekeningen, Lengkeek reglement, correspondentie met OR).
- Gesprekken met medewerkers (met name bestuurders, leden van de OR, het hoofd IT, hoofd personeelszaken en de controller van Lengkeek).
- Gesprekken met derden (NIVRE).
- Systemen voor digitale gegevensopslag (met name LAS).

Middels het literatuuronderzoek is gekeken welke eisen de huidige privacywetgeving in Nederland stelt aan de verwerking, opslag en beveiliging van persoonsgegevens. Welke gegevens mogen verwerkt worden en welke niet? Wie mag bepaalde gegevens beheren en inzien? Welke mate van beveiliging schrijft de wet voor? Wanneer de voorschriften van de wet duidelijk zijn zal de huidige situatie bij Lengkeek hier aan worden getoetst.

Het doel van dit onderzoek is een rapport aan te leveren dat eventuele kritische punten binnen Lengkeeks privacybeleid benoemt, maar ook kan dienen als handleiding voor toekomstige vraagstukken over hoe om te gaan met privacy issues binnen de organisatie. De door OR en bestuurders aangedragen probleempunten zullen dus de kern zijn van een breder georiënteerd onderzoek.

³ Mr. H.H. de Vries, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 17.

2 - De Wbp & persoonsgegevens

Bijna iedereen die gegevens over personen verzamelt of gebruikt, heeft te maken met de Wbp. Bij het verwerken van deze gegevens spelen veel elementen een rol waaronder; de aard van de gegevens, het doel van het gebruik en de mate waarin door dat gebruik de persoonlijke levenssfeer van de betrokkene wordt aangetast. Daarom zal in dit hoofdstuk worden ingegaan op de wet en enkele belangrijke termen. Eerst zal echter kort gekeken worden naar de geschiedenis van privacy of 'het recht op bescherming van de persoonlijke levenssfeer'. Ook de WPR en de internationale wetgeving komen hierbij aan bod teneinde te verduidelijken hoe de huidige wetgeving tot stand is gekomen.

2.1 Geschiedenis

De ontwikkeling van het recht op bescherming van de persoonlijke levenssfeer kwam halverwege de twintigste eeuw op gang.⁴ Een van de weinige positieve gevolgen van de Tweede Wereldoorlog is namelijk de grote aandacht voor mensenrechten. Het recht op bescherming van de persoonlijke levenssfeer is een van deze rechten en is dan ook terug te vinden in enkele belangrijke internationale stukken.

In de UVRM, aangenomen door de VN in 1950, is het recht opgenomen in artikel 12 welke luidt:

- *Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet.*

De UVRM is, zoals de naam zegt, slechts een verklaring en niet juridisch bindend. Daarom bepaalde de VN in artikel 17 van het in 1969 door Nederland ondertekende IVBPR het volgende:

- *Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.*
- *Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.*

Ook het EVRM waarborgt dit recht in soortgelijke bewoordingen in artikel:

- *Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*
- *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 economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.*

⁴ J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk (4^e druk)*, Deventer: Kluwer 2007, p. 9.

Op nationaal niveau leidde een advies van de staatscommissie Cals/Donner in 1983 tot het invoeren van meerdere sociale grondrechten waaronder een privacyrecht.⁵ Artikel. 10 van de grondwet bepaalt sindsdien het volgende:

- *Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.*
- *De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.*
- *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.*

Het recht op privacy is dus stevig verankerd in zowel internationale als nationale regelgeving. De eerste moderne privacywet in Europa was die van de West-Duitse deelstaat Hessen in 1970. Zweden was het eerste land dat overging tot het invoeren van een algemene privacywet in 1973. In 1978 creëerden Frankrijk, Noorwegen, Denemarken en Oostenrijk hun privacywetten. Daarna volgden Luxemburg (1979), IJsland (1981) en het Verenigd Koninkrijk (1984).⁶ De verschillende privacy wetten in de verschillende landen leverden vooral voor ondernemingen lastige situaties op bij grensoverschrijdend gegevensverkeer. Een bekend voorbeeld is het verbod personeelsgegevens van Siemens-Zweden over te brengen naar het hoofdkwartier in München in verband met het gebrek aan equivalente privacybescherming in de Bondsrepubliek.⁷

De eerste aanleidingen voor de totstandkoming van privacywetgeving in Nederland waren de algemene volkstelling van 1970 en de ontwikkeling van een centrale personenadministratie op basis van een algemeen persoonsnummer.⁸ Het was ook in die periode dat de toename van computergebruik, waarmee persoonsgegevens werden opgeslagen, leidde tot nationale groeiende privacyonrust.⁹ Er werd een staatscommissie ingesteld die moest bepalen of er privacywetgeving tot stand moest komen. Het eindrapport van deze 'commissie-Koopmans' bevatte al een uitgebreid voorontwerp van wet. Toch duurde het nog jaren tot de WPR in 1989 in werking trad. De WPR is de voorloper van de huidige Wbp en ondervond veel kritiek. Deze nieuwe wet zou te star zijn en weinig compatibel met de snelle ontwikkelingen op het gebied van ICT in die tijd. Er was ook veel discussie betreffende de toezichthouder in het WPR tijdperk, de zogenaamde Registratiekamer. Bij de vervanging van de WPR door de Wbp heeft de wetgever getracht de zwakke punten uit de WPR op te vangen.¹⁰ Ook is er momenteel de mogelijkheid het handelen van de nieuwe toezichthouder, het CBP, te toetsen bij de Nationale Ombudsman.

2.2 EU-privacyrichtlijn

Zoals hierboven al besproken, wordt de bescherming van de burger tegen inbreuken op zijn persoonlijke levenssfeer door democratische staten op waarde geschat. Wanneer ieder land echter zijn eigen regels opstelt kan dit een remmend effect hebben op de internationale handel. Dit probleem in combinatie met het toenemende grensoverschrijdend gegevensverkeer, versterkt door een revolutie in de ICT, leidde ertoe dat de EU haar

⁵ J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk (4^e druk)*, Deventer: Kluwer 2007, p. 11.

⁶ J.E.J. Prins & J.M.A. Berkvens, *Privacyregulering in theorie en praktijk (2^e druk)*, Deventer: Kluwer 2000, p. 40.

⁷ J.E.J. Prins & J.M.A. Berkvens, *Privacyregulering in theorie en praktijk (2^e druk)*, Deventer: Kluwer 2000, p. 38.

⁸ J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk (4^e druk)*, Deventer: Kluwer 2007, p. 13.

⁹ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 14.

¹⁰ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 15.

‘Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens’ opstelde.¹¹

De richtlijn kwam uiteindelijk pas in 1995 formeel tot stand.

Richtlijnen moeten door de lidstaten binnen een bepaalde tijd geïmplementeerd worden in hun nationale wetgeving. Zo kwam in Nederland in 2001 de huidige Wbp tot stand die de WPR vervangt.¹² De richtlijn bepaalt voor een groot deel de inhoud van de nationale wetgeving. Er wordt daarom verder niet ingegaan op de bepalingen in de richtlijn maar direct overgegaan op de Wbp.

2.3 Terminologie uit de Wbp

De Wbp bevat regels over het verwerken van persoonsgegevens. Met ‘verwerken’ wordt het gehele proces van het moment van verzameling van een gegeven tot vernietiging bedoeld. De ICT heeft er toe geleid dat opgeslagen gegevens met het grootste gemak, en in enorme hoeveelheden, kunnen worden verspreid via allerlei netwerken. Er is specifiek gekozen voor de formulering ‘het verwerken van persoonsgegevens’ omdat deze zin vrij technologie-neutraal is.¹³ De huidige formulering vangt de gehele verwerking dus goed op in welke zin dan ook. De Wbp is in eerste plaats van toepassing op geautomatiseerde verwerking van persoonsgegevens, maar ook op handmatige verwerking indien die gegevens opgenomen zijn in een bestand of bestemd zijn om daarin opgenomen te worden.

Een ‘bestand’ is een gestructureerd geheel van gegevens dat betrekking heeft op verschillende personen. De gegevens moeten onderlinge samenhang vertonen en systematisch toegankelijk zijn.¹⁴ Een enkel ongestructureerd handmatig personeelsdossier valt dus niet onder de Wbp. Een gealfabetiseerde rij uniform opgebouwde dossiers in een dossierkast weer wel.

Voorbeelden van verwerken zijn niet alleen het opslaan en ordenen van gegevens. Ook het verzamelen, bewaren en verstrekken aan derden vallen onder het begrip. Zelfs het vernietigen of afschermen van gegevens is een verwerking op zich. Een belangrijke voorwaarde bij het verwerken van persoonsgegevens is dat de verwerker feitelijke macht moet uitoefenen over de persoonsgegevens. ‘Feitelijke macht’ is een ingewikkeld begrip. Er hoeft geen sprake te zijn van menselijke tussenkomst om van feitelijke macht te spreken. Ook volledig geautomatiseerde vormen van verwerkingen kunnen onder de Wbp vallen. Het gaat erom dat de mogelijkheid tot enige invloed aanwezig is.¹⁵ Een voorbeeld:

Wanneer een Telecom operator gegevens simpelweg doorvoert verwerkt hij geen persoonsgegevens en is de Wbp niet van toepassing. Wanneer diezelfde operator de mogelijkheid heeft gegevens in te zien en te ordenen is de mogelijkheid tot invloed aanwezig en verwerkt hij persoonsgegevens in de zin van de Wbp (ook al maakt hij geen gebruik van die mogelijkheid).

Dan rest de vraag wat een ‘persoonsgegeven’ is. In de Wbp wordt dit omschreven als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het gegeven moet dus informatie verschaffen over een persoon. Logische gegevens zijn iemands naam, adres of burgerservicenummer, maar ook een foto, iemands opvattingen of

¹¹ Richtlijn 1995/46/EG (PbEG 1995 L 281/31).

¹² J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk (4^e druk)*, Deventer: Kluwer 2007, p. 13.

¹³ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 17.

¹⁴ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 18.

¹⁵ T.F.M. Hooghiemstra, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: SDU uitgevers 2007, p. 36.

zelfs gedragingen kunnen persoonsgegevens zijn. Hier onder enkele voorbeelden van (mogelijke) persoonsgegevens:¹⁶

- Telefoon/computergebruik.
- Benzineverbruik van een leaseauto.
- Ziekteverzuim of redenen daarvan.
- Productieaantallen.
- Toetsaanslagen op de computer.
- Overzicht van gevolgde cursussen en opleidingen.
- De unieke nummers van Wifi-routers.¹⁷

Wanneer een gegeven iemand wel of niet identificeerbaar maakt verschilt. Het is in ieder geval niet zo dat wanneer gegevens ontdaan worden van direct herleidbare gegevens als naam, adres en woonplaats, er per definitie geen sprake meer is van identificeerbaarheid.¹⁸

Men kan in veel gevallen uit een combinatie van andere gegevens iemand alsnog identificeren.

Belangrijke spelers binnen de Wbp zijn de verantwoordelijke, de betrokkene en de bewerker. Deze termen worden nu verder toegelicht.

2.4 Betrokkene

De betrokkene is degene op wie een gegevensverwerking betrekking heeft. In Lengkeeks geval dus de werknemers, klanten/opdrachtgevers, en ieder ander wiens persoonsgegevens door Lengkeek verwerkt worden.

2.5 De verantwoordelijke

Wie de verantwoordelijke is, is veel lastiger te bepalen. Conform artikel 1 sub d Wbp is de verantwoordelijke:

- *De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.*

Het is belangrijk dat duidelijk is wie de verantwoordelijke binnen een organisatie is omdat de betrokkene moet weten wie aanspreekbaar is voor de verwerking van zijn gegevens.¹⁹

Verantwoordelijke is diegene die formeel-juridisch de bevoegdheid heeft om doel en middelen van de persoonsgegevensverwerking te bepalen.²⁰ Degene die feitelijk het doel van en de middelen voor de gegevensverwerking bepaalt is daarmee niet per definitie de verantwoordelijke in de zin van de Wbp. Om voor Lengkeek te bepalen wie nu verantwoordelijke is moet worden aangesloten bij het civielrechtelijke personen- en organisatierecht.

Lengkeek, Laarman & de Hosson bestaat als maatschap. Binnen deze rechtsvorm zijn het natuurlijke personen die het doel van, en de middelen voor de verschillende vormen van

¹⁶ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 19.

¹⁷ College Bescherming Persoonsgegevens, Beslissing op bezwaar 22 juli 2011 Google inc./Google Netherlands B.V. (<www.cbppweb.nl>)

¹⁸ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 19.

¹⁹ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 19.

gegevensverwerking vaststellen. Men onderscheidt in het algemeen de volgende drie vormen van verantwoordelijkheid in de zin van de Wbp:²¹

1) *Gemeenschappelijke verantwoordelijkheid*

Hoewel verschillende entiteiten deelnemen aan de verwerking van de persoonsgegevens wordt er een enkele verantwoordelijke specifiek benoemd. Deze persoon wordt naar buiten toe aangewezen als verantwoordelijke en is zodanig ook aansprakelijk. Ondertussen blijven de afzonderlijke entiteiten verantwoordelijk voor de door hen aangeleverde gegevens. De gemeenschappelijke verantwoordelijke is verantwoordelijk voor de inhoud hiervan voor zover hij over dat deel van de gegevens juridische zeggenschap heeft.

2) *Gedifferentieerde verantwoordelijkheid*

Iedere verantwoordelijke is verantwoordelijk voor de door hem verwerkte gegevens. Er is geen gemeenschappelijk aangewezen verantwoordelijke en de betrokkene die zijn rechten wil invoeren moet zich dus richten tot specifiek die verwerker die voor zijn gegevens verantwoordelijk is.

3) *Gezamenlijke verantwoordelijkheid*

Meerdere partijen zijn gezamenlijk verantwoordelijk voor verschillende verwerkingen die geïntegreerd zijn. Er is geen gemeenschappelijk aangewezen verantwoordelijke. Iedere verantwoordelijke die een gegevensbestand heeft aangeleverd is aansprakelijk voor het geheel van de gegevensverwerkingen.

Bovenstaande vormen zijn niet limitatief. Wie de verantwoordelijke is en hoe dit bepaald moet worden is vaak omstreden en onduidelijk. In die gevallen zal, naar de in het maatschappelijk verkeer geldende maatstaven, beoordeeld moeten worden wie verantwoordelijk is voor een gegevensverwerking.²²

Binnen Lengkeek is geen persoon aangewezen als gemeenschappelijke verantwoordelijke voor de gegevensverwerking. De melding bij het CBP (zie hoofdstuk 5) die gewoonlijk door de verantwoordelijke wordt gedaan, is in 2006 gedaan door firmant Cees van Scherpenzeel. In de melding is 'Lengkeek, Laarman & De Hosson' opgegeven als verantwoordelijke. Dhr. Van Scherpenzeel geeft zelf aan dat hij niet als verantwoordelijke beschouwd dient te worden. Hij geeft aan dat er één iemand zou moeten zijn die zich bezig houdt met compliance.

Omdat er niemand specifiek is aangewezen als verantwoordelijke en ook niemand de verantwoordelijkheid specifiek gedelegeerd heeft gekregen is er waarschijnlijk sprake van een gezamenlijke verantwoordelijkheid. In dit geval is de directie van Lengkeek dan verantwoordelijke in de zin van de Wbp, totdat iemand anders uitdrukkelijk tot verantwoordelijke wordt benoemd. Zo is bijvoorbeeld de afdeling Personeelszaken, die nieuwe werknemers gegevens laat invullen, en deze ordent in kasten, toch niet verantwoordelijke in de zin van de Wbp.

2.6 De bewerker

Lengkeek besteedt een groot deel van haar personeelsregistratie uit aan het salaris- en personeelsadministratiebedrijf ADP. ADP is in deze verhouding een klassiek voorbeeld van een bewerker. Zoals al eerder vermeld is de verantwoordelijke diegene die het doel en de middelen van de gegevensverwerking vaststelt. Het verschil tussen de verantwoordelijke en

²¹ E. Thole, F. Van der Jagt & H. Roerdink, 50 vragen over privacy, Deventer: Kluwer 2010, p. 35.

²² E. Thole, F. Van der Jagt & H. Roerdink, 50 vragen over privacy, Deventer: Kluwer 2010, p. 36.

de bewerker is dat de laatste geen zeggenschap over de gegevensverwerking heeft.²³ De bewerker handelt naar de instructies en onder de verantwoordelijkheid van de verantwoordelijke. Toch staat een bewerker nooit onder het gezag van een verantwoordelijke. Werknemers in dienst van een verantwoordelijke kunnen dan ook nooit bewerkers zijn. Een bewerker mag de persoonsgegevens die hij verwerkt ook niet voor eigen doeleinden gebruiken. Wanneer hij dit wel doet is hij namelijk verantwoordelijke.²⁴ Artikel 1 sub e van de Wbp bepaalt het volgende:

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

Omdat het wat betreft de personeelsregistratie duidelijk is dat ADP bewerker en Lengkeek verantwoordelijke is, en ADP dat ook zelf aangeeft in art. 6 van haar algemene voorwaarden, zal hier nu niet verder op worden ingegaan. Wel is het van belang te vermelden dat ADP als bewerker verantwoordelijk is voor schade die iemand lijdt voor zover deze het gevolg is van haar bewerkingshandeling. ADP moet in een dergelijk geval aantonen dat de schade haar niet kan worden toegerekend.²⁵ Ook rusten de geheimhouding en beveiligingsverplichting op ADP, maar de meldingsplicht en het informeren van betrokkenen weer op Lengkeek. Op bovenstaande plichten wordt later in dit rapport dieper ingegaan.

De werknemers van Lengkeek verwerken de gegevens van hun eigen klanten in het systeem. Omdat het personeelsleden zijn, en zij dus in een hiërarchische positie staan tot de verantwoordelijke, kunnen zij wettelijk geen bewerker zijn en is hier sprake van zogenaamd 'intern beheer'.²⁶

2.7 Reglement en gedragscode

Het Lengkeek reglement bevat secundaire arbeidsvoorwaarden en andere afspraken en regels ter aanvulling op de individuele arbeidsovereenkomst. Ook zijn er enkele regels te vinden die aansluiten op het onderwerp privacy. Artikel 9b van het Lengkeek reglement bepaalt dat iedere gebruiker zich dient te realiseren dat het intranet een eenvoudig toegankelijk systeem is waarin geen enkele vorm van privacy kan worden gegarandeerd. De werkgever neemt echter in principe geen kennis van de inhoud van zowel zakelijke als niet zakelijk e-mails. Gegevens over internetgebruik, bezochte sites en tijdsbesteding worden evenmin geregistreerd. Wel kunnen controles op incidentele basis vanwege zwaarwichtige redenen plaatsvinden. Feitelijk blijkt dat de gegevens omtrent e-mail en internetgebruik wel worden geregistreerd, maar niet bekeken, een essentieel verschil.

Uit de 'Gedragscode expertiseorganisaties' blijken verder geen specifieke bepalingen betreffende privacy. Op zijn hoogst kan gesteld worden dat de bepalingen over professionaliteit, vertrouwen en integriteit aansluiten bij een correct privacybeleid.

Lengkeek is aangesloten bij de Kamer van het Nederlands Instituut van Register-Experts (NIVRE). Binnen Lengkeek Expertises zijn Register-Experts werkzaam, ingeschreven bij het NIVRE. Uit contact met het NIVRE blijkt dat zij hun leden geen speciale eisen of richtlijnen betreffende privacy opleggen.

Lengkeek beschikt over een ISO 9001/2008 certificaat. Deze norm stelt eisen aan kwaliteitsmanagementsystemen die door een organisatie gebruikt kunnen worden. Deel van de norm zijn zowel voldoen aan de eisen van de klant als aan die van de wet- en

²³ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 109.

²⁴ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 109.

²⁵ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 110.

²⁶ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 109.

regelgeving. Zodoende is er wel een (zwakke) link te leggen tussen privacy en ISO 9001/2008 in de zin dat aan de wet voldaan dient te worden. Voor informatiebeveiliging bestaan echter aparte ISO normen die zich geheel op het onderwerp richten (ISO 27001 & 27002).

3 - De gegevensverwerking binnen Lengkeek

In dit hoofdstuk zal worden bekeken welke werknemer- en klantgegevens binnen Lengkeek worden verwerkt en of het gaat om persoonsgegevens of niet. Dit hoofdstuk beperkt zich tot de automatische en handmatige gegevensverwerkingen die bestemd zijn om opgenomen te worden, of al opgenomen zijn, in een bestand. Zoals gezegd is een persoonsgegeven conform art. 1 sub a Wbp: 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'.

De automatische gegevensverwerking van klantgegevens vindt plaats in het digitale systeem LAS. De digitale personeelsgegevens in ADP blijven buiten beschouwing maar van alle in de systemen opgenomen gegevens zijn ook fysieke dossiers aanwezig in kasten en lades. Dan zijn er nog aparte programma's waarin tankgedrag, parkeergedrag, mailgedrag, surfgedrag, belgedrag en deurregistratie wordt bijgehouden. Ook de internetsite en het intranet van Lengkeek bevatten werknemersgegevens. Het softwareprogramma OQM waarin het kwaliteitsmanagementsysteem van Lengkeek is vastgelegd en de 'openbare mappen' in het Outlook mailsysteem bevatten ook werknemersgegevens.

Van belang is vervolgens dat de gegevensverwerkingen behoorlijk en zorgvuldig zijn. De gegevens mogen slechts verzameld worden voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden.²⁷ Art. 8 Wbp somt de gronden op die een gegevensverwerking rechtvaardigen:

Persoonsgegevens mogen slechts worden verwerkt indien:

- a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
- b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
- c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
- d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
- e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
- f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert

Voor Lengkeek zijn verschillende van deze gronden van toepassing.

Tot slot verdient het nog vermelding dat de gegevens die worden doorgespeeld naar de Arbodienst, Centraal beheer Achmea en Nationale Nederlanden buiten beschouwing worden gelaten.

3.1 Fysieke werknemersgegevens

Aard: De fysieke werknemersgegevens die Lengkeek verwerkt bestaan uit die gegevens die door een nieuwe werknemer ingevuld worden op een gestandaardiseerd formulier van de afdeling Personeelszaken. Het is overduidelijk dat het hier gaat om gegevens waaruit een individu direct te identificeren valt (naam, adres, burgerservicenummer, telefoon, bankgiro, opleidingen, titels etc..). Het gaat dus om persoonsgegevens in de zin van de Wbp. De

²⁷ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 22.

gegevens worden ook opgenomen in een gestructureerd bestand, namelijk zowel een fysieke opslag (kast) bij Personeelszaken in Rotterdam, als digitaal in ADP.

Doel: Het doel van het verwerken van deze gegevens is het uitvoeren van de arbeidsovereenkomst. Ook meer algemeen het contact met de werknemer en het voldoen aan enkele wettelijke verplichtingen.

Grondslag: De grondslagen die hier van toepassing zijn, zijn het nakomen van wettelijke verplichtingen (8 sub c Wbp) en het uitvoeren van de arbeidsovereenkomst (8 sub b Wbp). De verwerking is daarmee gerechtvaardigd.

3.2 Lengkeek Automatiserings Systeem (LAS)

Aard: In LAS worden informatie betreffende de klant en ook uiteindelijke schade- en/of taxatierapporten ingevoerd. Het startscherm van LAS bevat al naam, adres en e-mailgegevens. Ook het bankgiro- en telefoonnummer van klanten is in LAS te vinden. Ook hier is dus sprake van persoonsgegevens in de zin van de Wbp.

Doel: Het doel hier is een zo goed en compleet mogelijk beeld te krijgen van de toedracht, omvang en hoogte van de schade en de daarbij betrokken personen. Deze doelen vloeien deels voort uit wettelijke verplichtingen en deels uit het gerechtvaardigde belang van Lengkeek.

Grondslag: Er kan gesteld worden dat er sprake is van toestemming van de betrokkene voor de verwerking (8 sub a Wbp). Bij het aangaan van de verzekeringsovereenkomst accepteerde hij immers ook de verplichting informatie te moeten afgeven bij een eventuele claim. Ook is het een gerechtvaardigd belang van Lengkeek om de gegevens nodig voor een effectieve en juiste bedrijfsvoering op te slaan (8 sub f Wbp).

3.3 Fysieke klantgegevens (dossiers)

Aard: De fysieke dossiers van Lengkeeks klanten bevatten naam, adres, postcode telefoonnummer en gedetailleerde informatie over het voorval waaruit de getaxeerde schade ontstaan is, bijvoorbeeld een diefstal. Vaak is ook een proces-verbaal in het dossier bijgevoegd. Over het algemeen zal er een overeenkomst zijn tussen gegevens in het LAS bestand en het fysieke dossier. Er kan dus geconcludeerd worden dat het wat betreft de inhoud van Lengkeeks fysieke dossiers om persoonsgegevens in de zin van de Wbp gaat. Het doel en de grondslag zijn gelijk aan die zoals besproken in 3.2.

3.4 Werknemersgegevens buiten ADP

Hieronder worden alle soorten werknemersgegevens besproken die buiten ADP vallen.

Belgegevens

Aard: Lengkeek beschikt over de mobiele belgegevens van haar werknemers via een door Telfort gecreëerde online nota. De administratie kan online inloggen en een bestand downloaden waar namen en nummers in staan met de specifieke belkosten en belinformatie. Dat er hier sprake is van identificeerbaarheid en persoonsgegevens in de zin van de wet is dus duidelijk.

Doel: Het doel ligt in het geval van Lengkeek bij kosten- en capaciteitsbeheersing. Het is zaak dat werknemers niet buitensporig veel onkosten maken en/of de telefoon gebruiken voor privé doeleinden.

Grondslag: De grondslag in deze is het gerechtvaardigde belang van de verantwoordelijke (art. 8 sub f Wbp) om de telefoonkosten die de medewerkers maken in de hand te houden. Lengkeek betaalt immers de rekeningen.

Deurregistratie

Aard: De deurregistratie wordt alleen in Eindhoven en Rotterdam bijgehouden in de digitale programma's 'Cardaces' en 'Timewize'. Daarin kan de administrator op naam zien wanneer iemand in- en uitloopt. Op die manier wordt duidelijk hoe vaak iemand op kantoor is geweest

en hoelang. De administrator heeft inzicht in die gegevens. Het hele kantoor heeft inzicht in of iemand 'binnen' is of niet. Dit laatste is vooral van belang voor secretaresses. Omdat de gegevens van de deurregistratie ook per werknemer individueel te bekijken zijn is ook hier sprake van persoonsgegevens. De Amsterdamse vestiging heeft geen deurregistratie en de vestiging in Zwolle gebruikt nog een pasjessysteem dat de vorige gebruiker van het pand hanteerde waarmee geen gegevens worden opgeslagen.

Doel: Het doel is de beveiliging van het gebouw en het scheppen van een veilige werkomgeving voor zowel personeel als bedrijfsinformatie. De deurregistratie werkt als digitaal slot. Ook speelt een efficiënte bedrijfsvoering hier een rol. Elke werknemer kan zelfstandig het gebouw in. Het doel is niet gelegen in de aan- en afwezigheidsregistratie of urenregistratie terwijl het systeem dit wel mogelijk maakt.

Grondslag: Het gerechtvaardigd belang van Lengkeek. Lengkeek is verantwoordelijk voor de veiligheid van haar medewerkers en de informatie die zich binnen het gebouw bevindt. Een open deurbeleid zou niet passend zijn.

E-mail gegevens

Aard: Lengkeek heeft de mogelijkheid op een server in te loggen en alle e-mail gegevens van haar werknemers per individu te bekijken. De gegevens zijn dan voor de administrator op eenzelfde manier beschikbaar als voor de betrokkene.

Doel: Het doel ligt in dit geval bij kosten- en capaciteitsbeheersing. Eventueel ook nog het bekijken of de regels binnen het bedrijf worden nageleefd.

Grondslag: De grondslag is het gerechtvaardigd belang van Lengkeek. Het is van belang dat werknemers niet grote hoeveelheden tijd besteden aan privé zaken via de mail of het internet (sociale netwerken bijvoorbeeld). Ook kan gegevensbescherming hier een rol spelen.

Internet gegevens

Aard: Het programma IWSS (Interscan Websecurity Suite) biedt een zogenaamd 'specific user report'. Hierin zijn per werknemer de gegevens over het internetgebruik te vinden. Op de voet van de wettelijke definitie van persoonsgegevens, kunnen ook email- en internet gegevens zo worden gekwalificeerd.²⁸ Bij e-mail is in ieder geval sprake van verwerking als gegevens worden opgeslagen, bewaard, geordend, beschermd, uitgewist of vernietigd. Omdat bij e-mailverkeer altijd wel één van deze handelingen (eventueel door software) wordt verricht is er hier ook sprake van verwerking in de zin van de Wbp. Het 'specific user report' over het internetgebruik wijst ook op precieze identificatie van de gegevens per gebruiker en valt dus ook onder de Wbp.

Doel en grondslag: Dezen zijn in dit geval gelijk aan die bij het e-mailgebruik.

Camera's

Aard: Het camera toezicht bij de toegangsdeuren is vrij beperkt. Alleen de vestigingen Zwolle en Rotterdam hebben een deurcamera waarmee op een beeldscherm kan worden bekeken wie voor de deur staat. Deze persoon kan dan via de deurintercom binnen worden gelaten. Essentieel hierbij is dat de camera geen informatie opslaat (er zijn geen recorders aangesloten op de camera's). Er is dus geen sprake van opname in een 'bestand'. Omdat de wet ziet op de verwerking van persoonsgegevens die in een bestand worden opgenomen valt het camera toezicht buiten de reikwijdte van de Wbp.

²⁸ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 76.

Parkeergegevens

Aard: Met Park-line parkeren werknemers van Lengkeek hun auto's met hun mobiel. Aan het eind van de maand rekent Park-line via automatisch incasso of Creditcard de kosten af. De gegevens die bij deze handeling door Lengkeek ontvangen worden zijn het kenteken in combinatie met de initialen van de werknemer en de parkeerinformatie (tijd en plaats).

Doel: Het doel is in dit geval beheersing van de parkeerkosten.

Grondslag: Het gerechtvaardigd belang van Lengkeek om de parkeerkosten van haar werknemers in de hand te houden.

Tankpassen

Aard: De tankpassen van de twee door Lengkeek gebruikte leasemaatschappijen (Athlon en Leaseplan) verschaffen veel informatie. Door in te loggen krijgt Lengkeek inzicht in gegevens over het verbruik, soort auto, bijtellingspercentages, tankgedrag (waar en wanneer), kilometerstand en bekeuringen.

Doel: In analogie met de parkeer- en telefoonkosten gaat het hier om beheersing van de brandstofkosten.

Grondslag: De grondslag is het gerechtvaardigd belang van de werkgever om de kosten in de hand te houden. Er worden hier echter wel meer gegevens opgeslagen dan voor de doelstelling nodig zijn.

Internet & intranet

Aard: Zowel op Lengkeeks internetsite als intranet staan foto's van alle werknemers met de naam, telefoonnummer en email (werk), de vestiging en afdeling waar de werknemer werkt en zijn of haar functie binnen die afdeling. Ook zijn de specialismen van de werknemer nog aangegeven. Op het intranet staan nog enkele extra gegevens zoals het thuisadres, mobiel nummer, geboortedatum en datum van indiensttreding.

Doel: Persoonlijke benaderbaarheid van de organisatie voor derden, en transparantie naar buiten toe wat betreft de competenties van werknemers. De informatie op het Intranet dient als een interne communicatieversterking.

Grondslag: Wat het internet betreft is de enige (en tamelijk zwakke) grondslag die hier van toepassing is de ondubbelzinnige toestemming van de werknemer. In een arbeidsverhouding is 'ondubbelzinnige toestemming' meestal een zwakke grondslag omdat de werknemer in een hiërarchische verhouding tot de werkgever staat en hij zodoende het gevoel kan krijgen dat geen toestemming geven nadelige gevolgen kan hebben. Voor de gegevens op het intranet speelt het gerechtvaardigd belang van de werkgever (soepele interne communicatie) wel weer een rol.

Openbare mappen

Aard: In de interne 'openbare mappen' van het Outlook mailsysteem staan nog enkele contactgegevens van (oud) werknemers en een agenda met verjaardagen.

Doel en grondslag: Doel en grondslag zijn hier in principe hetzelfde als die hierboven voor het intranet zijn beschreven. Het valt dan ook aan te bevelen de werknemersgegevens in de 'openbare mappen' geheel te verwijderen omdat dezelfde gegevens ook op het intranet staan. De administrator van Lengkeek geeft ook aan dat de meeste persoonsgegevens al zijn verwijderd uit de openbare mappen omdat het intranet daar nu voor wordt gebruikt.

OQM kwaliteitsmanagementsysteem

Aard: In OQM staan gedetailleerde functieomschrijvingen van de werknemers met naam, e-mail, nevenfuncties en tekenbevoegdheden. Verder staan de taken van verschillende werknemers beschreven met hun opleidingen en specialismen erbij.

Doel: Het doel is interne communicatieversterking en duidelijkheid over een ieders functie en bevoegdheden. Ook speelt transparantie over eventuele nevenfuncties een rol. Een uitgebreid beschreven kwaliteitsmanagement is ook van belang voor de ISO certificatie.

Grondslag: De grondslag is het gerechtvaardigde belang van Lengkeek om het kwaliteitsmanagement operationeel te hebben. Voor een efficiënte bedrijfsvoering is het van belang dat de namen van de werknemers erbij staan.

Er kan geconcludeerd worden dat, met uitzondering van de camera's in Rotterdam en Zwolle, de bovenstaande vormen van gegevensverwerking allen onder de Wbp vallen. De gegevens zijn stuk voor stuk alleen al via naam simpel te herleiden tot een betrokkene en zijn dus persoonsgegevens. Ook zijn alle gegevens opgenomen in een gestructureerd bestand zoals bedoeld in de Wbp. Het is dan ook overbodig nog naar de specifieke omstandigheden van gevallen te kijken.

Wel is van belang dat in het geval van de deurregistratie en de tankpassen meer gegevens worden verzameld dan nodig is voor het doel. In deze gevallen valt het aan te bevelen de overbodige gegevens niet meer te verzamelen of de doelen aan te passen aan de mogelijkheden van het systeem (en dit te communiceren richting werknemers). De werknemersgegevens op het internet worden verwerkt onder de zwakke grondslag 'ondubbelzinnige toestemming'. Het valt aan te bevelen een duidelijke procedure op te stellen waarin werknemers die toestemming geven. Op zichzelf is de grondslag in een arbeidsverhouding namelijk al zwak in verband met de hiërarchische verhouding tussen werkgever- en nemer.

Ook zouden de verschillende doelen expliciet omschreven moeten worden in een stuk (men zou kunnen denken aan het stuk bedoeld onder 4.4). Verder valt aan te bevelen om alle persoonsgegevens te verwijderen uit de openbare mappen, het intranet dient immers precies hetzelfde doel.

4 - Gegevensopslag en beveiliging

In dit hoofdstuk zal worden beschreven hoe de hiervoor vermelde gegevens worden opgeslagen en of dit conform de wet gebeurt. Er wordt dus ingegaan op de eisen die de Wbp stelt aan beveiliging van persoonsgegevens wat betreft digitale en fysieke opslagsystemen. Omdat de Wbp de beveiliging van gegevens weinig gedetailleerd omschrijft is ook het rapport *'beveiliging van persoonsgegevens'*, van de Registratiekamer in dit hoofdstuk van belang.²⁹ Hierin worden concretere handvaten gegeven over hoe verschillende typen gegevens te beschermen. De studie is gebaseerd op het bepaalde in artikel 13 Wbp en geeft richting aan hoe de verantwoordelijke met de beveiliging van persoonsgegevens dient om te gaan. Ook is de studie een uitgangspositie voor de privacy auditor om te bepalen in hoeverre de beveiliging adequaat is ingevuld.³⁰ De beveiliging van persoonsgegevens kent drie kwaliteitsaspecten.³¹

1) *Exclusiviteit*

Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.

2) *Integriteit*

De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.

3) *Continuïteit*

De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn in overeenstemming met de daarover gemaakte afspraken en de wettelijke voorschriften. Continuïteit wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.

Net als in de hiervoor genoemde studie zal ook in dit rapport ervan uit worden gegaan dat binnen Lengkeek, omwille van het bedrijfsbelang, de integriteit en continuïteit van de beveiliging voldoende gewaarborgd is. Dit hoofdstuk behandelt de exclusiviteit en er zal worden beschreven of en hoe bevoegdheden en rechten zijn verdeeld wat betreft de toegang tot verschillende gegevens.

Het vereiste niveau van beveiliging is direct afhankelijk van de risicoklasse van de gegevens, de stand van de techniek en de kosten van de implementatie van de maatregel.³² De te treffen maatregelen moeten worden afgestemd op bedreigingen die realistisch zijn gezien de aard van de persoonsgegevens in verhouding tot de omvang en de verwerkingen daarvan. Hierdoor wordt het risico van verlies of onrechtmatige verwerking tot een aanvaardbaar niveau beperkt. Bij het bepalen van de risicogevoeligheid spelen veel aspecten een rol waaronder de organisatie zelf, de aard, het doel en de omvang van de gegevensverwerking en de invloed daarvan op de maatschappelijke positie van de betrokkene. Ook de eventuele

²⁹ G.W. van Blarckom, J.J. Borking, *Beveiliging van persoonsgegevens*, achtergrond studies en verkenningen 23. Registratiekamer, 2001.

³⁰ G.W. van Blarckom, J.J. Borking, *Beveiliging van persoonsgegevens*, achtergrond studies en verkenningen 23. Registratiekamer, 2001, p 21.

³¹ G.W. van Blarckom, J.J. Borking, *Beveiliging van persoonsgegevens*, achtergrond studies en verkenningen 23. Registratiekamer, 2001, p8.

³² G.W. van Blarckom & J.J. Borking, *Beveiliging van persoonsgegevens*, Achtergrond studies en verkenningen 23, Registratiekamer april 2001, p. 15.

schade die de organisatie leidt door een onrechtmatige verwerking van persoonsgegevens speelt een rol.³³

4.1 Fysieke opslag

De dossiers van Lengkeeks klanten bestaan uit opgeslagen dossiers en dossiers die onder handen zijn. De opgeslagen dossiers worden in fysieke vorm geordend op factuurnummer en opgeslagen op de volgende manieren:

- Kasten op de vestigingen.
- Archiefunits op de vestigingen.
- Een aparte loods (voor de minder recente dossiers).
- Een kluis eenheid.
- Bij een extern bedrijf (Iron Mountain gegevens opslag).

De dossiers die onderhanden zijn bij werknemers liggen op de bureaus, bij werknemers thuis of worden meegenomen naar de klant.

Zoals gezegd is de Wbp alleen van toepassing op de niet geautomatiseerde gegevensverwerkingen die in een 'bestand' zijn opgenomen of bestemd zijn om daarin opgenomen te worden. Alle bovenstaande manieren van opslag vallen onder het begrip 'bestand' in de zin van de Wbp (gedefinieerd in art. 1 sub c Wbp). De opslag is namelijk geordend op factuurnummer en heeft betrekking op verschillende personen. De gegevens vertonen onderlinge samenhang en er is een uniforme chronologische en inhoudelijke opbouw van dossiers. Er is dus sprake van een systematisch toegankelijk en sterk gestructureerd systeem.³⁴ De dossiers die onderhanden zijn, zijn duidelijk bestemd om te worden opgenomen in het fysieke bestand en vallen dus ook onder de Wbp.

De loods en de externe opslag bij Iron Mountain genieten enige bescherming. De loods is afgesloten en de sleutel opgeborgen. Iron Mountain is een bedrijf dat zich specialiseert in het veilig opslaan van fysieke gegevens. Iron Mountain is bewerker en wordt in dit onderzoek buiten beschouwing gelaten om dezelfde reden als ADP. De opslagkasten op locatie, archiefunits en kluis eenheid zijn zowel onder werktijd als daarbuiten niet afgesloten.

4.2 Digitale opslag

Zoals vermeld in hoofdstuk 3 worden parkeer-, e-mail-, internet-, deurregistratie-, bel- en tankgegevens digitaal opgeslagen. De LAS, OQM- en Outlook systemen zijn vanzelfsprekend eveneens digitaal. Hieronder wordt kort doorgenomen hoe deze gegevens beschermd zijn en wie er toegang tot heeft.

Belgegevens

Om inzage te krijgen in het belgedrag logt de administrator met een gebruikersnaam en paswoord in op een online account van Telfort en downloadt de gegevens. Hij is de enige die toegang heeft tot de gegevens. Het gaat dan overigens alleen om mobiele belgegevens. Het gebruik van de vaste lijnen valt niet per individu te controleren.

Parkeergegevens

Ook voor de parkeergegevens wordt online ingelogd via een gebruikersnaam en paswoord. De enige die toegang tot de gegevens hebben zijn de afdeling Personeelszaken en de controller van Lengkeek.

³³ G.W. van Blarckom & J.J. Borking, *Beveiliging van persoonsgegevens*, Achtergrond studies en verkenningen 23, Registratiekamer april 2001, p. 23.

³⁴ H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001, p. 18.

Deurregistratie

In een aparte offline module van de programma's 'Cardacces' en 'Timewize' wordt ingelogd. Alleen de administrator en de afdeling Personeelszaken hebben hier toegang toe.

Tankgegevens

Alleen de controller kan online inloggen bij beide leasemaatschappijen (Athlon en Leaseplan). Hij gebruikt een inlogcode en bij Leaseplan is er daarbovenop nog een zogenaamde E-plan code vereist na het inloggen (dubbele beveiliging).

E-mail & internet

Gegevens over e-mail- en internetgebruik van werknemers worden verkregen na inloggen door de administrator in een intern systeem. Hij is de enige die hiertoe toegang heeft.

LAS

Binnen LAS zijn ten eerste verschillende bevoegdheden toegekend aan verschillende groepen medewerkers. In een overzicht van de verschillende rechten in LAS zijn de volgende groepen te onderscheiden:

- Administrator.
- Boekhouding.
- Personen die offertes maken.
- Binnendienst.
- Vakgroepmanagers.

Dan zijn er nog enkele rechten betreffende dossieraanpassingen, nota's en relatiebeheer die aan individuen zijn toegekend in plaats van aan groepen.

De LAS login van de medewerkers (met hun verschillende rechten en bevoegdheden) is gebonden aan de computer login. Met computer login wordt bedoeld de eigen gebruikersnaam en het paswoord dat iedere Lengkeek medewerker heeft waarmee hij op zijn werkcomputer inlogt. Het gebruik van LAS wordt niet per medewerker vastgelegd maar er wordt wel twee keer per dag een back-up gemaakt door servers die op iedere vestiging staan.

Ook is er een zogenaamde 'VPN verbinding' die versleuteld is waardoor mensen vanuit huis met LAS kunnen werken. De administrator autoriseert hiertoe mensen. Deze mensen krijgen dan een specifiek programma op hun computer en loggen daarmee in op de VPN server. Daarna loggen ze nogmaals in op een zogenaamde 'Terminal Server' en zitten ze in het Lengkeek Systeem. Een VPN netwerk is een manier om verbinding te maken met het (gesloten) kantoor netwerk via een openbaar netwerk (in dit geval internet). Op de technische inhoud van een VPN netwerk zal in dit rapport verder niet dieper worden ingegaan.

Intranet, OQM & Outlook openbare mappen

Logischerwijs hebben alle medewerkers van Lengkeek toegang tot deze systemen. De beveiliging vindt ook hier plaats via de computer login. Om het OQM systeem in te komen moet daarna nogmaals apart worden ingelogd met paswoord en gebruikersnaam. De systemen zijn van buiten Lengkeek ook alleen toegankelijk via 'VPN verbinding'. De Outlook openbare mappen zijn daarop een uitzondering. Op de Outlook openbare mappen wordt hierna niet meer ingegaan omdat eerder al is aanbevolen alle persoonsgegevens uit dit systeem te verwijderen.

4.3 Beveiliging in de wet

Nu duidelijk is wat Lengkeek doet aan beveiliging is van belang wat de wet hierover voorschrijft. Art. 13 van de Wbp is in dit kader in eerste instantie van belang en stelt:

- *De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*

Duidelijk is dat Lengkeek verantwoordelijk is om persoonsgegevens te beschermen tegen verlies en in het bijzonder tegen onrechtmatige verwerking. Er staan verder in de wet geen aanwijzingen over wát nu bijvoorbeeld een passend beveiligingsniveau is en hoe risico's van verwerking moeten worden ingeschat. De studie *'Beveiliging van persoonsgegevens'* van de Registratiekamer biedt hier enige uitkomst.

Om te beginnen is het vermeldenswaardig dat onder 'onrechtmatige verwerking' ondermeer onbevoegde kennisneming valt.³⁵ De technische en organisatorische maatregelen waarover het artikel spreekt moeten als volgt worden gezien:³⁶

- Technische maatregelen zijn de logische en fysieke maatregelen in en rondom de informatiesystemen zoals toegangscontroles, vastlegging van gebruik en back-up.
- Organisatorische maatregelen zijn maatregelen voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens zoals toekenningen, deling van verantwoordelijkheden en bevoegdheden, instructies, trainingen en calamiteitenplannen.

4.4 Beoordeling van beveiliging via risicoklassen

Dit rapport behandelt beveiliging aan de hand van een indeling van gegevensverwerkingen in risicoklassen zoals in hoofdstuk 4 van de studie *'Beveiliging van persoonsgegevens'* van de Registratiekamer uiteen wordt gezet. Dit rapport noemt vier verschillende risicoklassen waarvan er twee op Lengkeek van toepassing zijn. Risicoklasse 1 (basisniveau) is van toepassing wanneer het gaat om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie. Risicoklasse 2 (verhoogd risico) is van toepassing indien het gaat om persoonsgegevens die voldoen aan een van de hieronder gegeven beschrijvingen:

- De verwerkingen van bijzondere persoonsgegevens (zoals bedoeld in artikel 16 Wbp)
- De verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene;
- De gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering;
- Alle verwerkingen van persoonsgegevens die met het bovenstaande vergelijkbaar zijn.

Omdat binnen Lengkeek alle gegevens (zowel klasse 1 als klasse 2 gegevens) samen worden opgeslagen onder dezelfde beveiligingsmaatregelen hoeft hiertussen geen onderscheid gemaakt te worden en is klasse 2 van toepassing voor Lengkeek. Per risicoklasse zijn er veertien aandachtsgebieden betreffende beveiliging geformuleerd. Hieronder zullen alleen de aandachtsgebieden die voor Lengkeek van belang zijn een voor

³⁵ Kamerstukken II 1997/98 25 892, nr. 3, p. 98.

³⁶ G.W. van Blarkom & J.J. Borking, *Beveiliging van persoonsgegevens*, Achtergrond studies en verkenningen 23, Registratiekamer april 2001, p. 15.

een behandeld worden. Zodoende zal duidelijk worden in welke mate Lengkeek voldoet aan de beveiligingseisen die bij de risicoklasse 2 hoort.

1: beveiligingsplan/beleid

Het management van de organisatie dient het informatiebeveiligingsbeleid, inclusief het beleid ter zake van de beveiliging van persoonsgegevens vast te stellen en dit beleid binnen de organisatie uit te dragen. Binnen Lengkeek is er echter geen beleidstuk of document dat zo expliciet aandacht aan privacy besteed.

2: Administratief

Alle taken, bevoegdheden en verantwoordelijkheden voor het beheer van de persoonsgegevens, inclusief die van een beveiligingsfunctionaris, die regelmatig aan de verantwoordelijke rapporteert, dienen expliciet vast te worden gelegd. Hier is momenteel binnen Lengkeek nog geen sprake van.

3: Beveiligingsbewustzijn

Alle werknemers, inclusief de tijdelijke werknemers, dienen geïnstrueerd te zijn over het informatiebeveiligingsbeleid en de verantwoordelijkheden van de werknemers voor het beveiligen van persoonsgegevens dienen expliciet in de functieomschrijving of het arbeidscontract opgenomen te worden. Gedurende functioneringsgesprekken hoort het onderwerp dan ook aan de orde te komen. Ook op deze punten lijkt aanscherping wenselijk.

4: Eisen aan personeel

Bij de aanstelling dienen alle medewerkers (inclusief de tijdelijke) die met persoonsgegevens zullen gaan werken een geheimhoudingsverklaring te tekenen. Bij sollicitanten dient de juistheid van het curriculum vitae en controle van de identiteit plaats te vinden. Tijdelijke medewerkers dienen onder strikte schriftelijk overeengekomen voorwaarden toegang tot verwerkingen van persoonsgegevens te krijgen. Hieraan voldoet Lengkeek grotendeels. Enkel de omgang met tijdelijke medewerkers dient verbeterd te worden. Zij hebben direct dezelfde toegang als hun collega's met een vast contract.

5: Inrichting van de werkplek

De inrichting van de werkplek moet toestaan dat medewerkers veilig met persoonsgegevens kunnen werken. Dit is bij Lengkeek grotendeels het geval. Zoals vermeld wordt er gewerkt met persoonlijke paswoorden en screensavers die automatisch uitloggen. De beveiliging van de fysieke gegevensdragers (dossiers/USB sticks) is weliswaar gegarandeerd door het afgesloten gebouw, een clean desk-policy is toch aanbevelenswaardig.

6: ICT infrastructuur

De tekst in de studie is bij dit onderwerp vrij uitgebreid. De door Lengkeek toegepaste ICT infrastructuur is echter in overeenstemming met de eisen uit de studie. De toegekende bevoegdheden in de organisatie worden in een overzicht bijgehouden zoals beschreven onder 4.2. Wel is van belang dat wanneer een derde onderhoud zou plegen aan Lengkeeks ICT systemen, in het contract is vastgelegd dat er vertrouwelijk met gegevens wordt omgegaan. Onderhoud aan de ICT systemen wordt in Lengkeeks geval meestal verzorgd door de eigen administrator maar ook door het bedrijf AedifiComm. Punt van kritiek is dat het onderhoud door AedifiComm al geruime tijd plaatsvindt zonder formele vastlegging, laat staan een geheimhoudingsverklaring.

7: Toegangsbeheer

De verantwoordelijke dient aan te geven welke functionarissen toegang tot de persoonsgegevens mogen hebben. Tevens geeft de verantwoordelijke aan wie in de organisatie bevoegdheden voor het verwerken van persoonsgegevens mag toedelen.

Wat het digitale gedeelte aangaat is dit redelijk goed geregeld. De administrator is degene die binnen LAS bevoegdheden toekent aan verschillende medewerkers. Zoals onder 5.2 besproken hebben verschillende groepen werknemers verschillende bevoegdheden. Tot de fysieke gegevens, ordners en dossiers, heeft echter iedereen gelijke toegang. Zoals gezegd zitten de kasten niet op slot, met uitzondering van die waarin de personeelsgegevens worden opgeslagen. Ook is het zo dat het bevoegd gebruik van de persoonsgegevens nu afhankelijk is van toegangscontrole door gebruikersnaam en wachtwoord maar niet van het tijdstip en de apparatuur die gebruikt wordt om toegang te krijgen. Dit is wel een vereiste uit het rapport maar lijkt gezien de werkzaamheden van Lengkeek moeilijk uitvoerbaar.

8: Netwerken/Externe verbindingen

Er dient gebruik te worden gemaakt van de beveiligingsopties die de aanwezige netwerkkapparatuur en software bieden. Toegang tot en vanuit publiek toegankelijke netwerken zoals internet wordt uitsluitend gemaakt via algemeen erkende beveiligingsmaatregelen, zoals firewalls. De verantwoordelijke moet zorgen voor een adequate fysieke beveiliging tegen verlies van persoonsgegevens. Draadloze datacommunicatie geschiedt uitsluitend indien de persoonsgegevens versleuteld worden verzonden. Lengkeek maakt (zoals bijna ieder bedrijf) gebruik van een firewall. Ook worden er tweemaal per dag van het gehele LAS bestand back-ups gemaakt. De inlogmogelijkheid buiten het interne netwerk om verloopt via een (beveiligde) VPN verbinding en is dus in orde.

9: Software van derden

Lengkeek maakt gebruik van software van ADP. Zoals gezegd garandeert ADP zelf dat zij voldoen aan alle relevante wetgeving evenals de door haar geleverde software. Verder wordt er in dit onderzoek van uitgegaan dat Lengkeek ook voor alle andere applicaties gebruik maakt van software die origineel en legitiem is.

10: Bulkverwerking

Geautomatiseerde bulkverwerking van persoonsgegevens is niet van toepassing op Lengkeek.

11: Bewaren van persoonsgegevens

De gegevensdragers met persoonsgegevens dienen in een afgesloten ruimte, voorzien van een inbraakdetectie te worden bewaard. Zoals gezegd zijn de gebouwen van Lengkeek afgesloten en voorzien van een alarm.

Ook mogen er geen gegevensdragers met persoonsgegevens onbeheerd worden achter gelaten op algemeen toegankelijke plaatsen. Een opmerking die hierbij gemaakt kan worden is dat na werktijd de open kasten en dossiers op de bureaus wel toegankelijk zijn voor personen die toegang tot het gebouw hebben, zoals bijvoorbeeld de schoonmakers. In principe zijn de schoonmakers geen vertrouwd personeel dat onder contract staat bij Lengkeek zelf. Het lijkt daarom niet goed dat deze mensen zulke vrije toegang hebben tot de informatie. Een oplossing hiervoor zou kunnen zijn de kasten te voorzien van sloten (vanzelfsprekend in combinatie met een clean desk-policy).

12: Vernietiging van persoonsgegevens

Het vernietigen van persoonsgegevens nadat de bewaartermijn is verlopen moet zorgvuldig gebeuren. Lengkeek laat fysieke gegevens vernietigen door een gespecialiseerd bedrijf. Het valt aan te bevelen dat Lengkeek van deze vernietigingen ook een administratie bijhoudt. Verder is het belangrijk dat digitale gegevensdragers als usb-sticks, harde schijven, cd-roms en dergelijke gewist worden voordat ze weggegooid worden.

13: Calamiteitenplan

De bewaarlocatie van back-ups moet zich buiten de locatie waar de verwerking van persoonsgegevens plaatsvindt bevinden. Voor de fysieke dossiers is dit natuurlijk niet haalbaar. Aangezien Lengkeek digitale back-ups van het gehele digitale LAS systeem op verschillende vestigingen draait is de veiligheid van de gegevens tegen calamiteiten gewaarborgd. De back-ups worden ook iedere dag meegenomen en dus buiten het kantoor bewaard.

14: Bewerkers

Lengkeek maakt gebruik van de bewerkers ADP en Iron Mountain. In hoofdstuk 1 is dit aspect uitgesloten van dit onderzoek. Conform de studie van de Registratiekamer is het wel belangrijk dat Lengkeek als verantwoordelijke zich regelmatig op de hoogte laat stellen van het beveiligingsniveau bij de bewerkers. Een keer per jaar zou dan voldoen.

5 - Lengkeeks rechten en plichten

Om transparantie te creëren ten aanzien van de gegevensverwerking en te waarborgen dat de gegevens zorgvuldig en behoorlijk worden verwerkt zijn in de Wbp aan de betrokkene verschillende rechten toegekend. In dit hoofdstuk worden enkele van die rechten beschreven die voor Lengkeek van belang zijn. Ook wordt ingegaan op de plichten die voor de verantwoordelijke voortvloeien uit de Wbp.

5.1 Meldingsplicht CBP

De Wbp schrijft een algemene meldingsplicht voor. Wie persoonsgegevens verwerkt moet dit melden bij het CBP en wel voordat wordt begonnen met de verwerking. De melding bevat tenminste de volgende informatie:

- Naam en adres van verantwoordelijke.
- Doel of doeleinden van de verwerking
- Doel of doeleinden waarvoor de (categorieën van) gegevens zijn of worden verzameld
- Beschrijving van de categorieën van betrokkenen en de gegevens die daarop betrekking hebben
- Categorieën van ontvangers aan wie de gegevens verstrekt kunnen worden.
- Een algemene beschrijving om een voorlopig oordeel te kunnen geven over de gepastheid van de voorgenomen veiligheidsmaatregelen.

Het is belangrijk te vermelden dat een melding bij het CBP niets te maken heeft met de inhoudelijke goedkeuring van de verwerking. Meestal controleert het CBP alleen of de melding compleet is en plaatst ze deze in een openbaar register (met uitzondering van informatie over de beveiliging).³⁷ Wanneer niet gemeld wordt terwijl dit wel moet kan dit resulteren in een geldboete.

Om de administratieve belasting bij het CBP te beperken en te voorkomen dat een overvloed aan irrelevante meldingen plaatsvindt, heeft de wetgever een ruim 'Vrijstellingsbesluit Wbp' gepubliceerd. Hierin worden de meeste standaard gegevensverwerkingen, noodzakelijk voor normale niet privacygevoelige bedrijfsvoering, uitgesloten van meldingsplicht aan het CBP.

Lengkeek heeft haar gegevensverwerking in 2006 gemeld bij het CBP onder meldingsnummer 1316760; de melding is eenvoudig te vinden in de openbare registers op de site van het CBP.³⁸ Deze melding is vrij gelimiteerd in omvang en inhoud en beperkt zich tot een brede vorm van cliënteninformatie, die enkel het expertise gedeelte behelst en zich niet bezighoudt met de pre-risk onderdelen van Lengkeek (bouwkundige opnames en taxaties). Daarnaast wordt ook geen melding gemaakt van het opslaan van gedetailleerde 'gebruiksgegevens' zoals e-mail-, internet-, tank-, deurregistratie- en telefoongegevens. De eenmalige melding aan het CBP is in 2006 verricht. Veranderingen in verwerking dienen echter wel direct (voor de start van de verwerking) aangemeld te worden.

Tot slot moet nog vermeld worden dat het Schiedammer adres dat in de melding staat incorrect is. De vestiging is inmiddels verhuisd naar Rotterdam. Het valt aan te bevelen deze wijziging direct door te geven aan het CBP omdat wijzigingen in de naam of het adres van de verantwoordelijke normaliter binnen een week dienen te worden doorgegeven. Wijzigingen in overige delen van de verwerking dienen binnen één jaar na de voorafgaande melding te worden doorgegeven.

³⁷ Mr. Drs. D. Rijkers, Privacy, *De Wet Bescherming Persoonsgegevens (Adfo Juridische Aspecten)*, Alphen aan den Rijn: Kluwer 2002, p. 73.

(<www.cbpreg.nl>) → openbare registers → register meldingen → zoeken → Lengkeek

De bij de wet aangewezen categorie verwerkingen die specifieke risico's meebrengt voor de rechten en vrijheden van de betrokkene is aan preventief toezicht door het CBP onderhevig.³⁹ Voor Lengkeek is in dit kader alleen de categorie 'verwerking van strafrechtelijke of daarmee gelijk te stellen gegevens ten behoeve van derden' van belang. Hieronder enkele voorbeelden:

- *Bij het aangaan van de verzekeringsovereenkomst heeft de verzekeringnemer een mededelingsplicht ten opzichte van de verzekeraar over feiten en omstandigheden die met de verzekeringsovereenkomst samenhangen (art. 7:928 BW). Wanneer daar uitdrukkelijk door de verzekeraar naar wordt gevraagd en wanneer strafbare feiten niet langer dan acht jaren vóór het sluiten van de verzekeringsovereenkomst zijn gepleegd moeten ook mededelingen worden gedaan over het strafrechtelijk verleden van de verzekerde. (art. 7:928 lid 5 BW). Dit leidt dan bijvoorbeeld tot andere voorwaarden, hogere premie of eventueel afwijzen van de verzekering. Niet zelden verzwijgt de verzekerde in dit kader zijn strafrechtelijk verleden. Vaak komt de Lengkeek-expert er bij de schadebehandeling uiteindelijk toch achter dat er iets aan de hand is. Afhankelijk van het strafrechtelijk verleden van een verzekerde hoeft de verzekeraar eventueel niet uit te keren. Via de expert belandt strafrechtelijke informatie over de verzekerde in dit proces bij Lengkeek.*
- *Lengkeek verzorgt ook regres. Bij strafbare feiten bijvoorbeeld, neemt de verzekeraar de schade over van de benadeelde, maar ook het recht die schade te verhalen op de veroorzaker. Bij het goed afhandelen van het regres m.b.t. een strafbaar feit komt Lengkeek al gauw in het strafrechtelijke proces terecht. Zo zal voor het verhalen van de schade vaak een vonnis nodig zijn. Deze gegevens belanden zodoende ook in de dossiers van Lengkeek.*

Een voorafgaand onderzoek naar de rechtmatigheid van de voorgenomen verwerking is in deze gevallen dus verplicht. Bij de uiteindelijke melding van dit type gegevens moet ook weer vermeld worden dat het gaat om gegevens waarvoor voorafgaand onderzoek vereist is. De verwerking mag dan niet plaatsvinden tot het onderzoek voltooid is, of het CBP heeft laten weten dat geen onderzoek verricht zal worden.⁴⁰

5.2 Melding aan medewerkers

Naast de hierboven genoemde meldingsplicht richting het CBP dient de verantwoordelijke uiteraard altijd betrokkenen te informeren over het gebruik van zijn persoonsgegevens. In de volgende gevallen is het noodzakelijk de medewerkers van Lengkeek expliciet te informeren over de aard van de verwerking, de mogelijkheid van controle en de rechten die de medewerker heeft (zie 5.3 en verder):

- Het controleren van e-mail en internetgebruik.
- Het opslaan en controleren van mobiele telefoongegevens.
- Het opslaan van gedetailleerde gegevens uit de deurregistratie (hiervoor heeft Lengkeek geen doel en grondslag).
- Het opslaan van tank- en parkeergegevens.

Daarnaast is nog van belang dat e-mailverkeer tussen OR leden niet gecontroleerd mag worden voor zover het OR gerelateerde kwesties betreft.

³⁹ D Mr. Drs. D. Rijkers, Privacy, *De Wet Bescherming Persoonsgegevens (Adfo Juridische Aspecten)*, Alphen aan den Rijn: Kluwer 2002, p. 74.

⁴⁰ Mr. Drs. D. Rijkers, Privacy, *De Wet Bescherming Persoonsgegevens (Adfo Juridische Aspecten)*, Alphen aan den Rijn: Kluwer 2002, p. 75.

5.3 Inzagerecht

Het inzagerecht houdt in dat een betrokkene zich altijd kan wenden tot Lengkeek met het verzoek hem mede te delen of er persoonsgegevens over hem worden verwerkt en welke dat dan zijn. Lengkeek dient deze informatie binnen vier weken na een dergelijk verzoek schriftelijk te overleggen aan de betrokkene.

Wanneer er daadwerkelijk gegevens worden verwerkt over die betrokkene, dient Lengkeek een volledig overzicht te verschaffen van die gegevens. Dit overzicht moet ook in begrijpelijke vorm worden verstrekt. Tot slot moet Lengkeek hierbij aangeven:⁴¹

- Wat de doeleinden van de verwerking zijn.
- De categorieën van gegevens waarop de verwerking betrekking heeft.
- De ontvangers van de gegevens.
- De beschikbare informatie over de herkomst van de gegevens.

Het verdient opmerking dat Lengkeek dergelijke verzoeken niet mag negeren, op zijn beurt mag de betrokkene zulke verzoeken ook niet te vaak doen.

Lengkeek mag voor verstrekking van deze informatie € 0,23 in rekening brengen per pagina tot een maximum van € 4,50 per verzoek. Wanneer het grote of moeilijk toegankelijke stukken betreft kan de vergoeding oplopen tot € 22,50.⁴²

5.4 Recht op correctie

Wanneer blijkt dat de persoonsgegevens waarover Lengkeek beschikt niet correct of onvolledig zijn kan de betrokkene altijd verzoeken de gegevens te corrigeren, aan te vullen, te verwijderen of beter af te schermen.⁴³ Het moet dan gaan om gegevens die:

- Feitelijk onjuist zijn.
- Voor het doeleind van de verwerking onvolledig of niet ter zake dienend zijn.
- In strijd met een wettelijk voorschrift zijn.

De betrokkene zal dan in zijn verzoek zelf moeten aangeven welke aanpassingen hij wenst. Over het algemeen wordt aangenomen dat de verantwoordelijke de correctie moet uitvoeren ook zonder dat eerst een verzoek als bedoeld in 5.3 heeft plaatsgevonden.⁴⁴ Lengkeek heeft ook na een correctieverzoek weer vier weken de tijd om schriftelijk te laten weten of ze voldoet aan het ingediende verzoek. Een afwijzing tot correctie dient door Lengkeek deugdelijk gemotiveerd te worden. Wanneer wel tot correctie wordt overgegaan moet dit zo snel mogelijk gebeuren.

Nadat gecorrigeerd is, is Lengkeek verplicht ook alle derden die de onjuiste informatie hebben ontvangen hierover te informeren, tenzij dit onmogelijk blijkt of onevenredige inspanning kost.⁴⁵ Dit laatste is echter zelden het geval, men moet hierbij denken aan opname van de gegevens in een groot landelijk adressenbestand zoals het telefoonboek of het handelsregister waarbij het vrijwel onmogelijk te achterhalen is wie van de gegevens gebruik hebben gemaakt.

5.5 Recht op Verzet

Het spreekt vanzelf dat een betrokkene zich mag verzetten in geval van verwerking van gegevens op onrechtmatige grondslag. Echter, ook in geval van verwerking op rechtmatige grondslag kan een betrokkene zich verzetten tegen een verwerking van zijn persoonsgegevens.

In het algemeen zijn er twee soorten verzet: relatief verzet en absoluut verzet.

⁴¹ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 49.

⁴² E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 50.

⁴³ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 50.

⁴⁴ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 51.

⁴⁵ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 52.

Absoluut verzet

Dit treedt enkel op in geval van gebruik van gegevens voor “direct marketing” en is dus niet van toepassing op de situatie bij Lengkeek. In geval van absoluut verzet wordt er van uitgegaan dat het gerechtvaardigd individueel belang van de betrokkenen zwaarder weegt dan dat van de verantwoordelijke.

Relatief verzet

In tegenstelling tot een groot aantal andere Europese lidstaten kent Nederland slechts een beperkt recht van relatief verzet. In Nederland is dit verzet alleen mogelijk bij gegevensverwerking op een van de volgende rechtvaardigingsgronden uit art. 8 Wbp:⁴⁶

- Noodzakelijkheid voor de vervulling van een publiekrechtelijke taak.
- Noodzakelijkheid voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke.

Omdat deze tweede grondslag binnen Lengkeek regelmatig voorkomt is deze vorm van verzet voor Lengkeek het meest relevant. Het verzet kan worden uitgeoefend als de betrokkene een gerechtvaardigd individueel belang heeft tegen de verwerking en dit belang ook kan aantonen.⁴⁷ De verantwoordelijke die verwerkt op de grondslag ‘gerechtvaardigd belang’ heeft immers altijd de afweging gemaakt tussen zijn belang om te verwerken en dat van de betrokkene op bescherming van zijn persoonlijke levenssfeer. Toch kan het zo zijn dat die afweging anders had moeten uitvallen in een individueel geval omdat de verantwoordelijke zich bijvoorbeeld niet bewust was van een bepaalde omstandigheid. Indien verzet wordt aangetekend moet de verantwoordelijke binnen vier weken beoordelen of het verzet terecht is.⁴⁸ Voor het in behandeling nemen van het verzet kan een vergoeding worden gevraagd van € 4,50 (welke teruggegeven wordt wanneer het verzet terecht blijkt).

5.6 Bewaartermijn

Een persoonsgegevensverwerking mag niet voor altijd door blijven gaan. Artikel 10 Wbp stelt namelijk:

- Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.
- Persoonsgegevens mogen langer worden bewaard dan bepaald in het eerste lid voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt

In principe blijkt uit deze tekst dat door de verantwoordelijke per geval moet worden bekeken welke bewaartermijn moet worden gehanteerd.

⁴⁶ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 52.

⁴⁷ Mr. Drs. D. Rijkers, *Privacy, De Wet Bescherming Persoonsgegevens (Adfo Juridische Aspecten)*, Alphen aan den Rijn: Kluwer 2002, p. 63.

⁴⁸ Mr. Drs. D. Rijkers, *Privacy, De Wet Bescherming Persoonsgegevens (Adfo Juridische Aspecten)*, Alphen aan den Rijn: Kluwer 2002, p. 64.

Klantgegevens (LAS en fysiek)

Lengkeek slaat dossiers na afwikkeling momenteel standaard op voor een periode van zeven jaar.⁴⁹ Deze termijn is in overeenstemming met de belastingwetgeving. In principe mag Lengkeek enkel de fiscaal relevante gegevens zeven jaar bewaren en dient het bedrijf de overige gegevens waar mogelijk eerder te vernietigen. Lengkeek heeft er (vermoedelijk uit praktische overwegingen) voor gekozen om alle gegevens zeven jaar te bewaren en daarna te vernietigen. Het lijkt ook ondoenlijk om alleen de fiscale gegevens uit alle dossiers te selecteren. Bovendien is het ook nog zo dat klanten van Lengkeek worden geïnformeerd over de bewaartermijn en deze soms zelf ook verlangen.

Personeelsgegevens (ADP en fysiek)

De persoonsgegevens in het personeelsbestand blijven opgeslagen, ook nadat de werknemer afscheid heeft genomen van Lengkeek. De salarisadministratie die van fiscaal belang is dient weer zeven jaar bewaard te worden. De loonbelastingverklaring en het identiteitsbewijs dienen minstens vijf jaar bewaard te blijven. Voor alle andere informatie geldt een richtlijn van twee jaar (of vernietiging zoveel eerder als mogelijk is).⁵⁰

Gebruiksgegevens (parkeren, telefoon, tanken, e-mail, internet, toegang)

De informatie over het parkeren, tanken, de deurregistratie en het e-mail- en internetgebruik worden nooit verwijderd. Het CBP heeft echter aangegeven dat het bewaren van de e-mail gegevens in principe beperkt moet worden tot het bewaren van de verkeersgegevens (afzender, datum en tijd van bericht) en dat deze maximaal zes maanden bewaard mogen worden.⁵¹ Indien Lengkeek de gegevens langer wil bewaren is melding bij het CBP vereist. Op grond van de door het CBP voor e-mail gegeven richtlijn van zes maanden bewaartermijn, lijkt het redelijk en aanbevelenswaardig voor Lengkeek om deze bewaartermijn ook in acht te nemen voor de andere bovengenoemde gebruiksgegevens.

5.7 Rol van de OR

Wat betreft het onderwerp privacy is in de praktijk met name art. 27 lid 1 sub l en sub k WOR van belang voor de OR. Hier wordt een instemmingsrecht bepaald ten aanzien van een aantal besluiten die van invloed kunnen zijn op de privacy en het verwerken van persoonsgegevens.⁵² Het artikel luidt:

De ondernemer behoeft de instemming van de ondernemingsraad voor elk door hem voorgenomen besluit tot vaststelling, wijziging of intrekking van:

- ***k. Een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen;***
- ***l. 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.***

De rechten van de OR hebben geen invloed op de eerder genoemde individuele rechten van de werknemers. Een werknemer kan zich dus wel degelijk verzetten tegen een door de OR goedgekeurde verwerking. Het goed betrekken van de OR toont wel aan dat de werkgever rekening houdt met de belangen van zijn werknemers. Dit kan bijvoorbeeld bij de rechter een rol spelen wanneer deze moet beoordelen of er een zorgvuldige belangenafweging is gemaakt.⁵³

⁴⁹ Dit is ook zo bepaald binnen kwaliteitsmanagementsysteem OQM.

⁵⁰ (<www.cbppweb.nl>) → Nieuws en publicaties → informatiebladen → Informatieblad: bewaartermijnen van persoonsgegevens in uw bestanden p. 3.

⁵¹ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 191.

⁵² E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 206.

⁵³ E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010, p. 206.

Het is belangrijk te onderkennen dat alle personeelsvolgsystemen onder art. 27 lid 1 sub I WOR vallen. Dus ook de systemen die Lengkeek gebruikt voor bijvoorbeeld deurregistratie, e-mail en internetcontrole.

Lengkeek moet een voorgenomen besluit tot het in gebruik nemen van zulke systemen schriftelijk en deugdelijk gemotiveerd aan de OR voorleggen. De OR heeft vervolgens instemmingsrecht. Als de OR die instemming op oneigenlijke gronden onthoudt, kan Lengkeek de kantonrechter om vervangende toestemming vragen. Besluiten die instemmingsplichtig zijn en zonder instemming van de OR worden genomen zijn nietig.

6 - De Wet Harrewijn en de maatschap Lengkeek

De Wet Harrewijn, genoemd naar het in het voorjaar van 2002 overleden Tweede Kamerlid Ab Harrewijn, is een uitbreiding van het informatierecht van de OR en komt neer op het invoegen van twee artikelen in de WOR (31d/31e). De wijziging houdt kortweg het volgende in: minstens een keer per jaar moet de werkgever aan de ondernemingsraad ongevraagd schriftelijke informatie geven over de beloningsstructuur en de inhoud van de arbeidsvoorwaarden en afspraken per verschillende groep werknemers in het bedrijf. Hierbij hoort ook informatie over het salaris en de aanvullende arbeidsvoorwaarden van directie, bestuurders en toezichthouders.

De hoofdvraag in dit hoofdstuk is of de wet wel of niet op Lengkeek van toepassing is. Voor de volledigheid zal echter ook kort worden ingegaan op de link tussen privacy en de Wet Harrewijn. Artikel 31d van de WOR luidt als volgt:

- 1. De ondernemer verstrekt, mede ten behoeve van de bespreking van de algemene gang van zaken van de onderneming, ten minste eenmaal per jaar aan de ondernemingsraad schriftelijk informatie over de hoogte en inhoud van de arbeidsvoorwaardelijke regelingen en afspraken per verschillende groep van de in de onderneming werkzame personen.*
- 2. De ondernemer verstrekt daarbij tevens schriftelijke informatie over de hoogte en inhoud van de arbeidsvoorwaardelijke regelingen en afspraken met het bestuur dat de rechtspersoon vertegenwoordigt en het totaal van de vergoedingen, dat wordt verstrekt aan het toezichthoudend orgaan, bedoeld in artikel 24, tweede lid.*
- 3. Ten aanzien van het eerste en tweede lid wordt inzichtelijk gemaakt met welk percentage deze arbeidsvoorwaardelijke regelingen en afspraken zich verhouden tot elkaar en tot die van het voorgaande jaar.*
- 4. Indien een groep, als bedoeld in het eerste lid, het bestuur of het toezichthoudend orgaan, bedoeld in het tweede lid, uit minder dan vijf personen bestaat, is het mogelijk om voor de toepassing van deze leden twee of meer functies samen te voegen, zodat een groep van ten minste vijf personen ontstaat.*
- 5. De ondernemer is verplicht de ondernemingsraad zo spoedig mogelijk in kennis te stellen van belangrijke wijzigingen die in deze regelingen en afspraken worden aangebracht.*
- 6. Dit artikel is uitsluitend van toepassing op ondernemingen waarin in de regel ten minste 100 personen werkzaam zijn.*

Duidelijk is in ieder geval dat de uitsluitinggrond in lid 6 niet op Lengkeek van toepassing is omdat er momenteel ongeveer 150 personen binnen Lengkeek werkzaam zijn. Vervolgens is artikel 31 e WOR van belang welke enkele andere uitsluitingsgronden opsomt:

*Artikel **31d** is niet van toepassing op:*

- a. De besloten vennootschap met beperkte aansprakelijkheid waarvan een van de bestuurders of commissarissen een natuurlijk persoon is die een direct of indirect belang heeft in de rechtspersoon overeenkomstig artikel 4.6 van de Wet inkomstenbelasting 2001, of*
- b. De rechtspersoon waarop de artikelen 396 of 397 van titel 9 van Boek 2 van het Burgerlijk Wetboek van toepassing zijn.*

Het eerste sub van dit artikel is niet van toepassing op Lengkeek. Lengkeek heeft als juridische vorm de Maatschap (onderverdeeld in vier BV's). Dan rest sub b, dat enkele artikelen uit het burgerlijk wetboek noemt. Deze artikelen bepalen of een bedrijf sommige vrijstellingen geniet wat betreft het jaarrekeningenrecht. Mochten deze artikelen van toepassing zijn op Lengkeek dan sluiten zij in principe ook de toepasselijkheid van de wet Harrewijn uit. Wel dient opgemerkt te worden dat de maatschap in het huidige ondernemingsrecht geen rechtspersoon is. Dat zou de uitsluitinggrond eventueel kunnen ondergraven.

6.1 Artikel 2:396 BW

Dit artikel geldt alleen voor de rechtspersoon die op twee opeenvolgende balansdata aan enkele voorwaarden voldoet. Het artikel vindt toepassing als aan twee of drie van de volgende voorwaarden is voldaan:

- De waarde van de activa volgens balans met toelichting bedraagt op de grondslag van verkrijgings- en vervaardigingsprijs, niet meer dan € 4.400.000.
- De netto-omzet over het boekjaar bedraagt niet meer dan € 8.800.000.
- Het gemiddeld aantal werknemers over het boekjaar bedraagt minder dan 50.

Hieronder zijn de (afgeronde) gegevens over de boekjaren 2009/2010, zoals opgenomen in de gewaarmerkte jaarrekeningen die naar de OR zijn gestuurd, weergegeven.

2009

- Waarde activa € 7,4 miljoen
- Netto-omzet € 10,6 miljoen

2010

- Waarde activa € 7,2 miljoen
- Netto-omzet € 13 miljoen

2009/2010

- Het gemiddeld aantal werknemers blijkt niet uit de jaarrekeningen maar heeft altijd ruim boven de 50 gelegen.

Er kan geconcludeerd worden dat Lengkeek aan geen van de drie in 2:396 BW genoemde voorwaarden voldoet, het artikel geldt dus niet voor Lengkeek. Op die manier vindt de uitsluitingsgrond van 31e lid 2 WOR dan ook geen toepassing.

6.2 Artikel 2:397 BW

Ook dit artikel stelt voorwaarden die op twee opeenvolgende balansdata van toepassing moeten zijn. Dit artikel vindt ook weer toepassing als aan twee of drie van de volgende voorwaarden zijn voldaan:

- De waarde van de activa volgens balans met toelichting bedraagt op de grondslag van verkrijgings- en vervaardigingsprijs, niet meer dan € 17.500.000.
- De netto-omzet over het boekjaar bedraagt niet meer dan € 35.000.000.
- Het gemiddeld aantal werknemers over het boekjaar bedraagt minder dan 250.

Duidelijk is dat Lengkeek in dit geval aan alle drie de criteria voldoet en het artikel dus toepassing vindt. (Wat de laatste voorwaarde betreft heeft Lengkeek nooit meer dan 250 werknemers gehad). Via 2:397 vindt de uitsluitingsgrond van 31 e lid 2 WOR dus in principe toepassing en is 31 d WOR (de wet Harrewijn) niet op Lengkeek van toepassing.

Het lijkt erop dat het de wetgever met de Wet Harrewijn meer ging om de financieel economische en personele omvang van organisaties dan om de precieze juridische vorm (rechtspersoon of niet). Aldus kan geconcludeerd worden dat op grond van de financieel-economische en personele omvang van de maatschap Lengkeek het artikel genoemd in 31e lid b tot uitsluiting zou leiden. Het verdient wel opmerking dat het moeilijk in te schatten is hoe bij een meningsverschil hierover de Ondernemingskamer zal beslissen. Er is hierover nog geen jurisprudentie te vinden. Ook moeten bedrijven die onder de hierboven besproken vrijstelling vallen nog steeds de financiële informatie verstrekken zoals bepaald is in het '*Besluit verstrekking financiële informatie aan Ondernemingsraden 1985*'.

6.3 Privacy & de Wet Harrewijn

De privacy wetgeving en de Wet Harrewijn lijken wellicht met elkaar te conflicteren. Zeker wat betreft strategische bedrijfsinformatie of informatie over topinkomens die eventueel

onder de Wet Harrewijn verstrekt zou moeten worden. De Wet Harrewijn houdt rekening met het privacyaspect door in 31d lid 4 WOR de mogelijkheid te bieden gegevens te clusteren.⁵⁴ Kleine groepen personeel (van minder dan 5 personen) kunnen worden samengevoegd tot groepen van tenminste 5 personen. Deze regel lijkt voornamelijk in het leven te zijn geroepen voor de top van bedrijven, waar logischerwijs sneller een 'kleine groep' zal voorkomen.⁵⁵ Door de mogelijkheid tot clusteren wordt voorkomen dat uit informatie iemand direct identificeerbaar is en het dus zou gaan om persoonsgegevens.

⁵⁴ E. van der Cruijssen, R. Peters, *Wat verdient de top en wat krijgt de OR, een brochure voor or'en over beloningen in het bedrijf*, FNV pers, 2007, p.16

⁵⁵ E. van der Cruijssen, R. Peters, *Wat verdient de top en wat krijgt de OR, een brochure voor or'en over beloningen in het bedrijf*, FNV pers, 2007, p.16

7 - Conclusies en aanbevelingen

Centraal in deze scriptie staat de vraag in hoeverre Lengkeek voldoet aan eisen die de Wbp stelt aan de verwerking en opslag van persoonsgegevens. Op basis van dit onderzoek kunnen ter beantwoording van die vraag de volgende conclusies worden getrokken:

1. Bij gebrek aan een specifiek hiervoor aangewezen persoon is de directie van Lengkeek gezamenlijk verantwoordelijk voor de gegevensverwerking in de zin van de Wbp. De werknemers, klanten en een ieder ander wiens persoonsgegevens worden verwerkt zijn betrokkenen. Personeelsregistratiebedrijf ADP en Iron Mountain gegevensopslag zijn bewerkers in de zin van de Wbp. De manier waarop individuele werknemers binnen Lengkeek klantgegevens verwerken is aan te merken als intern beheer.
2. Uit de 'gedragscode expertiseorganisaties' blijken geen specifieke bepalingen betreffende privacy. Ook brancheorganisatie NIVRE stelt geen speciale eisen betreffende dit onderwerp. De ISO 9001/2008 certificatie stelt eisen aan kwaliteitsmanagement. Deel hiervan is ook voldoen aan wet en regelgeving. Dit is de enige, maar tamelijk zwakke, link met het onderwerp privacy.
3. Het Lengkeek reglement dat door de directie in overleg met de OR is vastgesteld bepaalt dat Lengkeek geen kennis zal nemen van de inhoud van zakelijke en niet zakelijke e-mails. Hetzelfde geldt voor internetgebruik en tijdsbesteding daaraan. Wel kunnen controles op incidentele basis vanwege zwaarwichtige redenen plaatsvinden. Deze bepaling uit het reglement is in principe in overeenstemming met de wet. Wel wordt letterlijk in het artikel gesteld dat registratie van internet- en e-mail gegevens niet plaats vindt terwijl dit wel zo is.
4. De fysieke werknemers- en klantgegevens, alsmede de digitale klantgegevens in LAS vallen allen onder de Wbp. Hetzelfde geldt voor gegevens over belgedrag, tankgedrag, parkeergegevens, e-mail en internetgebruik, deurregistratie en de gegevens van werknemers op OQM, openbare mappen en intra- en internet. Het camera gebruik valt niet onder de Wbp.
5. De vereiste rechtmatige grondslag voor verwerking van deze onder punt 4 genoemde gegevens is grotendeels in orde. Wat betreft de gegevens van werknemers op internet, met name foto's, is de enige grondslag echter de ondubbelzinnige toestemming van de werknemer. Dit is altijd een zwakke grondslag in een arbeidsverhouding. Ook worden wat betreft deurregistratie en tankpassen meer gegevens opgeslagen dan voor het doel nodig is.
6. De wet stelt voor de beveiliging van persoonsgegevens een redelijk open norm. De risicoklassen 1 en 2 uit de studie '*Beveiliging van persoonsgegevens*' van de Registratiekamer zijn het best op de gegevensverwerking binnen Lengkeek van toepassing.
7. Buiten de in aanbeveling 1, 3, 4, 5, en 11 genoemde punten is de beveiliging van de persoonsgegevens binnen Lengkeek in orde.
8. Lengkeek voldoet formeel welliswaar aan de meldingsplicht die de Wbp voorschrijft. Inhoudelijk is de melding echter vrij gelimiteerd in omvang; enkel het expertise gedeelte van Lengkeeks werkzaamheden wordt erin behandeld. Ook wordt geen melding gemaakt van het opslaan van verschillende gebruiksgegevens (e-mail, internet, telefoon). Tenslotte is in de melding een incorrect adres opgegeven.

9. Lengkeek verwerkt af en toe strafrechtelijke gegevens van betrokkenen, hetgeen onderhevig is aan preventief toezicht door het CBP. Er moet dus eigenlijk een voorafgaand onderzoek naar de rechtmatigheid van die verwerkingen plaatsvinden. De verwerking van dit soort gegevens mag eigenlijk niet plaatsvinden tot dit onderzoek voltooid is.
10. De OR heeft een instemmingsrecht wat betreft de personeelsvolgsystemen binnen Lengkeek. Het instemmingsrecht geldt ook wat betreft een eventuele toekomstige regeling zoals bedoeld in aanbeveling 1.
11. Artikel 31e sub b WOR, welke toepasselijkheid van de Wet Harrewijn uitsluit, is in principe op Lengkeek van toepassing. Lengkeek is echter juridisch gezien een maatschap en dus geen rechtspersoon. Dit gegeven zou de uitsluitingsgrond ondergraven. De onderzoeker is van mening dat het de wetgever met de Wet Harrewijn meer gaat om de financieel economische omvang van het bedrijf dan om de precieze juridische vorm. Er is op dit punt echter geen jurisprudentie te vinden en het is dus onzeker hoe de ondernemingskamer in deze zou besluiten.

Verder kunnen vanuit het onderzoek de volgende aanbevelingen worden gedaan:

1. Het management dient beleid vast te stellen ter beveiliging van persoonsgegevens en dit beleid te implementeren binnen de organisatie. Verantwoordelijkheden en bevoegdheden voor het beheer van persoonsgegevens dienen expliciet te worden vastgelegd. Ook in de functieomschrijving of het arbeidscontract van de werknemers dient expliciet aandacht te worden besteed aan het onderwerp informatiebeveiliging.
2. Scherp de melding bij het CBP aan, in het bijzonder op gebied van de pre-risk activiteiten en opslag van de gebruikersgegevens. Herstel de fout in de gedane melding.
3. Bij sollicitanten dient altijd het CV en de identiteit gecontroleerd te worden aan de hand van een geldig identiteitsbewijs. Ook moet bij tijdelijke medewerkers expliciet worden afgesproken hoe met informatiebeveiliging wordt omgegaan.
4. De inrichting van de werkplek is op beveiligingsgebied grotendeels in orde. Wel valt het aan te bevelen een 'clean desk-policy' in te stellen. In het bijzonder zouden aan het eind van de werkdag in ieder geval de dossiers moeten worden opgeborgen in afsluitbare kasten zodat ze niet meer onbeheerd op de bureaus liggen.
5. Een registratie bijhouden van de vernietiging van persoonsgegevens door het gespecialiseerde bedrijf dat dit momenteel doet. Ook is het belangrijk dat Lengkeek zich regelmatig (eens per jaar) op de hoogte laat stellen van het beveiligingsniveau bij de bewerkers die voor haar werken.
6. De medewerkers meer expliciet informeren over het feit dat controle op e-mail- en internetgebruik mogelijk is. Hetzelfde geldt voor de mobiele telefoongegevens en de tank- en parkeergegevens.
7. Betrokkenen hebben wat betreft hun persoonsgegevensverwerking een inzagerecht, een correctierecht en in sommige gevallen een recht tot verzet. Lengkeek dient haar werknemers te allen tijde te informeren over alle persoonsgegevensverwerkingen en over de bovengenoemde rechten die betrokkenen hebben.

8. Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is. Lengkeek slaat alle klantgegevens in verband met belastingwetgeving gedurende 7 jaar op waarna ze vernietigd worden. In principe moeten enkel de gegevens die fiscaal van belang zijn zolang worden opgeslagen. Alle andere gegevens zouden eerder verwijderd moeten worden. De salarisadministratie die een fiscaal belang dient behoort 7 jaar bewaard te worden, loonbelastingverklaring en identiteitsbewijs dienen minstens 5 jaar bewaard te blijven en voor alle andere informatie geldt een richtlijn van 2 jaar (of vernietiging zoveel eerder als mogelijk is).
9. De 'gebruiksgegevens' als telefoon-, e-mail- en internetgebruik, tank- en parkeer gegevens en deurregistraties worden in principe nooit verwijderd. Dit moet wel gebeuren. Het CBP geeft aan dat e-mail gegevens maximaal zes maanden bewaard mogen worden. Wil Lengkeek die gegevens langer bewaren dan is melding bij het CBP vereist. Op grond van de door het CBP voor e-mail gegeven richtlijn van zes maanden bewaartermijn lijkt het redelijk en aanbevelenswaardig om deze bewaartermijn ook in acht te nemen voor de andere bovengenoemde "gebruiksgegevens".
10. Heroverweeg doelen van het gebruik van persoonlijke werknemersinformatie (foto, telefoon, naam, vestiging, specialisatie, etc.) op het internet. Bepaal hierbij een procedure waarin werknemers duidelijk hun ondubbelzinnige toestemming hiertoe geven.
11. Zorg dat onbevoegden (bijv. schoonmaakpersoneel en andere aanwezigen die geen rol vervullen in de inhoud van dossiers) ook buiten werktijd geen toegang tot privacygevoelige informatie hebben. Ook valt het aan te raden met het bedrijf dat ICT onderhoud pleegt (AedifiComm) afspraken te maken over geheimhouding of vertrouwelijkheid. Momenteel werkt AedifiComm voor Lengkeek zonder enige formele vastlegging.
12. Verwijder de werknemersgegevens die nog opgeslagen zijn in de openbare mappen van e-mailsysteem Outlook. Het intranet wordt tegenwoordig gebruikt voor dezelfde doelen.

Literatuurlijst

Boeken:

- Onder redactie van mr. Corrie Ebbers, *Tekstuitgave Wet bescherming persoonsgegevens*, 's-Gravenhage: Reed Business 2008.
- D. Rijkers, *Privacy, De Wet Bescherming Persoonsgegevens (Adfo Juridische Aspecten)*, Alphen aan den Rijn: Kluwer 2002
- E. Thole, F. Van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010.
- G. Vermeulen, *Privacy en strafrecht*, Antwerpen/Apeldoorn: Maklu 2007.
- H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens, Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001.
- J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk (4^e druk)*, Deventer: Kluwer 2007.
- J. Nieuwenhuis, *Tussen privacy en persoonlijkheidsrecht*, Nijmegen: Ars Aequi Libri, 2001.
- J.E.J. Prins & J.M.A. Berkvens, *Privacyregulering in theorie en praktijk (2^e druk)*, Deventer: Kluwer 2000.
- K. Henrard, *Mensenrechten vanuit internationaal en nationaal perspectief*, Den Haag: Boom Juridische uitgevers 2006.
- M.J. Kroeze, L. Timmerman & J.B. Wezeman, *De kern van het ondernemingsrecht*, Deventer: Kluwer 2007.
- S.M. Huydecoper, *Wet Bescherming Persoonsgegevens en ICT*, Den Haag: SDU Uitgevers 2006.
- T.F.M. Hooghiemstra, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: SDU uitgevers 2007.

Losse stukken:

- College bescherming persoonsgegevens, *Privacy: checklist voor de ondernemingsraad*, CBP 2002.
- G.W. van Blarckom, J.J. Borking, *Beveiliging van persoonsgegevens, achtergrond studies en verkenningen 23*. Registratiekamer, 2001.
- E. Timmer, *Ondernemingsraad krijgt recht op informatie over topinkomens*, Pellicaan advocaten 2006.
- E. van der Cruisen, R. Peters, *Wat verdient de top en wat krijgt de OR, een brochure voor OR'en over beloningen in het bedrijf*, FNV pers, 2007.
- Kamerstukken II 1997/98 25 892

Elektronische bronnen:

- www.overheid.nl
- www.rechtspraak.nl
- www.cbpweb.nl
- www.lengkeek.nl
- www.nivre.nl
- www.bureauveritas.nl
- www.park-line.nl
- www.ironmountain.nl
- www.pellicaan.nl

Evaluatie

Het belang van goed gebruik van persoonsgegevens en het veiligstellen van de privacy van individuen staan op dit moment in de maatschappij behoorlijk in de belangstelling. De wetgeving is relatief nieuw en veel bedrijven en medewerkersorganisaties (OR) worstelen met het onderwerp. Het in deze stage uitgevoerde onderzoek heeft, door interpretatie van de bestaande wet- en regelgeving en toepassing van deze gegevens op de situatie van het bedrijf Lengkeek, zinvolle en nieuwe inzichten opgeleverd. Dezen inzichten geven vermoedelijk zowel management als medewerkersorganisaties handvatten voor praktisch handelen. Het resultaat van deze studie kon dan ook worden weergegeven in een helder hoofdstuk met conclusies en aanbevelingen.