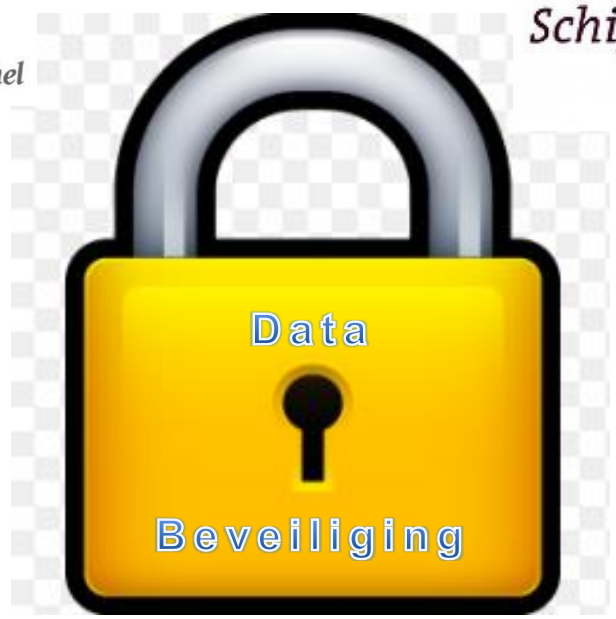
Praktijkgericht Juridisch Afstudeeronderzoek

Wet Meldplicht Datalekken en de Gemeente Meierijstad



Naam student:
Pelle Kuijs

Studentnummer Avans:
2057052

Stagedocent:
Wim Struijlaart

Stagementor Gemeente Veghel:
Ruud van Oorschot

Schijndel, 27 Mei 2016

Voorwoord

Ik heb dit onderzoek is uitgevoerd als onderdeel van mijn afstudeerstage bij de gemeente Veghel. Ik heb veel baat gehad bij de hulp van mijn stagementor Ruud van Oorschot en de ondersteuning van mijn stagedocent Wim Struijlaart. Ook wil ik graag Anke Hobbelen van de gemeente Sint-Oedenrode en Anouk Vlemmix van de gemeente Schijndel bedanken voor hun adviezen en assistentie. Tot slot wil ik nog mijn zus en mijn vader bedanken voor het kritisch doorlezen van mijn onderzoek, waardoor ik nog een aantal aanpassingen kon maken.

Inhoudsopgave

Samenvatting

Op 1 januari 2016 is de Wet Meldplicht Datalekken ingevoerd. Deze voert een meldplicht voor verwerkers van persoonsgegevens in bij het plaatsvinden van een datalek. De meldplicht is geïntroduceerd in de Wet Bescherming Persoonsgegevens en geldt zowel voor bedrijven, als voor decentrale overheden en semioverheidsinstellingen. Indien niet aan de meldplicht voldaan wordt kan de Autoriteit Persoonsgegevens een boete opleggen tot 820.000 euro. Dit betekent hoofdzakelijk dat er binnen bepaalde instellingen een procedure moet zijn voor het melden van een datalek en dat er maatregelen getroffen moeten worden om de kans op een datalek te minimaliseren.

De gemeenten Schijndel, Sint-Oedenrode en Veghel moeten ook voldoen aan deze vereisten. Een complicerende factor daarbij is dat deze drie gemeenten op 1 januari 2017 gaan fuseren tot de nieuwe gemeente Meierijstad. De gemeenten wilden dat onderzocht zou worden in hoeverre zij al voldoen aan de vereisten en waar ze op moeten letten bij het opstellen van een beleid omtrent datalekken binnen de nieuwe gemeente Meierijstad.

Methode

Om daar antwoord op te kunnen geven zijn de wet- en regelgeving, het gemeentelijk beleid en de gemeentelijke procedures omtrent databeveiliging en het melden van datalekken de primaire bronnen. Deze bronnen zijn geanalyseerd om mijn deelvragen te beantwoorden. Het onderzoek is opgedeeld in drie deelvragen met betrekking tot de wettelijke vereisten, het huidige beleid van de drie te fuseren gemeenten en de uitvoering hiervan.

Wettelijke vereisten

Allereerst is gekeken naar de wettelijke vereisten met betrekking tot databeveiliging en het melden van datalekken zoals beschreven in de Wet Bescherming Persoonsgegevens. Artikel 13 ziet toe op de beveiliging van persoonsgegevens en geeft aan dat de verantwoordelijke passende maatregelen ten uitvoer moet leggen om persoonsgegevens te beveiligen tegen ‘verlies of tegen enige vorm van onrechtmatige verwerking’. Artikel 34a ziet toe op het melden van datalekken. Dit artikel geeft aan dat de verantwoordelijke een inbreuk op de beveiliging, zo snel mogelijk moet melden aan de Autoriteit Persoonsgegevens indien deze leidt tot (de aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. In bepaalde gevallen moet een datalek ook gemeld worden aan diegene(n) wier persoonsgegevens zijn gelekt.

Beleid van de gemeenten

Alle drie de gemeenten hebben een beleid met betrekking tot het beveiligen van data. Deze beleidsstukken variëren in kwaliteitsniveau, maar voldoen alle drie wel aan de wettelijke vereisten. Daarentegen heeft geen van de drie gemeenten een beleid met betrekking tot het melden van datalekken dat voldoet aan de wettelijke vereisten.

Uitvoering van het beleid

Het beleid wordt binnen alle drie de gemeenten redelijk tot goed uitgevoerd. Vanwege de op handen zijnde fusie is het beleid van de gemeenten nog nergens volledig geïntegreerd, omdat dit inefficiënt zou zijn. Alle tijd die hier nu aan besteed wordt is namelijk verspild wanneer er binnen Meierijstad een nieuw beleid wordt gemaakt. Hoewel de meeste medewerkers van de drie te fuseren gemeenten weten dat er een databeveiligingsbeleid is, wordt er door minder dan 50 procent van de medewerkers iets mee gedaan.

Hoofdstuk 1: Inleiding

Op 1 januari 2017 gaan de gemeenten Schijndel, Sint-Oedenrode en Veghel fuseren tot de gemeente Meierijstad. Deze fusiegemeente zal een oppervlakte hebben van 185,52 vierkante kilometer en zal rond de 80.000 inwoners tellen. Hoewel op dit moment nog niet concreet is hoe de organisatie van de nieuwe gemeente eruit zal zien, zullen er in de gemeente waarschijnlijk rond de 500 mensen werkzaam zijn. Door deze fusie zullen er op veel gebieden nieuw beleid, nieuwe protocollen en nieuwe verordeningen opgesteld moeten worden. Zo ook met betrekking tot de Wet Meldplicht Datalekken.

De Wet Meldplicht Datalekken is op 1 januari 2016 ingevoerd. De Wet Meldplicht Datalekken is een wijzigingswet met betrekking tot het privacyrecht. De Wet Meldplicht Datalekken is ingevoerd nadat bij een groot aantal inbreuken op de beveiliging van onder andere websites als Ashley Madison, grote hoeveelheden persoonsgegevens op straat zijn komen te liggen.

Met de invoering van deze wet wordt vooral de Wet Bescherming Persoonsgegevens gewijzigd. Daarnaast vinden nog enkele kleine wijzigingen plaats in de Telecommunicatiewet, de Algemene Wet Bestuursrecht, de Wet Politiegegevens en de Wet Justitiële en Strafvorderlijke Gegevens. De Wet Meldplicht Datalekken heeft als voornaamste doel om een meldplicht in te voeren bij datalekken. Hierdoor zouden de gevolgen van een dergelijk datalek voor de betrokkene(n) beperkt kunnen worden.

Indien er een datalek is dient de verantwoordelijke voor de verwerking van persoonsgegevens dit volgens deze wet te melden bij de Autoriteit Persoonsgegevens (voorheen: College Bescherming Persoonsgegevens). Daarnaast dient de verantwoordelijke in bepaalde gevallen ook de betrokkene(n) op de hoogte te stellen. Het is mogelijk dat een betrokkene wiens data gelekt zijn door middel van een civiele procedure een schadevergoeding kan eisen. De verantwoordelijke kan ook door de Autoriteit Persoonsgegevens een boete opgelegd krijgen indien deze zijn data onvoldoende beveiligd, waardoor het datalek plaats heeft kunnen vinden of indien de verantwoordelijke heeft nagelaten om een datalek te melden. Een dergelijke boete kan tot 820.000 euro bedragen voor een gemeente. Ten slotte kan een groter datalek ook imago-schade voor de gemeente tot gevolg hebben.

Deze wet brengt voor gemeenten dan ook veel werk met zich mee. Niet alleen dient er een procedure opgesteld te worden voor datalekken, ook dienen de gemeenten het risico op datalekken zo veel mogelijk te verkleinen. Om die reden zijn vrijwel alle gemeenten in Nederland op dit moment druk bezig om aan deze wet te voldoen.

Ook de drie te fuseren gemeenten, Schijndel, Sint-Oedenrode en Veghel, en op termijn de fusiegemeente Meierijstad, zullen er voor moeten zorgen dat hun beleid en protocollen geschikt zijn om de kans op een datalek zo klein mogelijk te maken. Vanwege de op handen zijnde fusie tussen de drie gemeenten wordt hier nog een extra probleem aan toegevoegd. Het is namelijk de vraag hoe de protocollen en het beleid van de fusiegemeente Meijerijstad eruit moeten komen te zien. De drie te fuseren gemeenten hebben immers allemaal een verschillend beleid en verschillende protocollen op het gebied van databeveiliging. Dezen moeten dan ook beoordeeld worden om te kijken welke onderdelen uiteindelijk doorgevoerd worden in het beleid van de gemeente Meierijstad.

Naast de Wet Meldplicht Datalekken is er Europese wet- en regelgeving die toeziet op de bescherming van persoonsgegevens en de meldplicht van datalekken. De belangrijkste hiervan is de toekomstige Europese Algemene Verordening Gegevensbescherming, ook wel AVG genoemd.

§1.1 Doelstelling

Op 30 mei 2016 wordt een onderzoeksrapport opgeleverd aan de heer Ruud van Oorschot van de gemeente Veghel, met daarin aanbevelingen met betrekking tot de wet Meldplicht Datalekken in de gemeente Meierijstad en het huidige beleid van de drie te fuseren gemeenten met betrekking tot dit onderwerp. De drie te fuseren gemeenten kunnen door middel van deze informatie een beleid opstellen met betrekking tot de, uit de wet Meldplicht Datalekken voortgekomen, verplichtingen zodat het risico op datalekken en alle gevolgen van dien zo klein mogelijk is. Indien er alsnog een datalek ontstaat, moet deze op de juiste manier gemeld kunnen worden.

§1.2 Centrale vraag

In hoeverre zijn het beleid, de processen en de protocollen met betrekking tot databeveiliging en datalekken van de gemeenten Schijndel, Sint-Oedenrode en Veghel juridisch correct en voldoende doelmatig om opgenomen te worden in het toekomstige beleid, de processen en de protocollen van de fusiegemeente Meierijstad, gelet op de geldende wet- en regelgeving omtrent privacy?

§1.3 Onderzoeksmethodiek

Bij het schrijven van dit onderzoek is gelet op het gebruik van de juiste bronnen. De bronkeuze moet immers aansluiten op de aard van het onderzoek. Dit onderzoek is gericht op zowel de juridische als de praktische kant van de vraagstelling. De belangrijkste bronnen zijn de nationale en internationale wet- en regelgeving met betrekking tot het juridische gedeelte van het onderzoek en het gemeentelijke beleid en de gemeentelijke procedures met betrekking tot het praktische gedeelte van het onderzoek.

Om te beoordelen of de gemeentelijke procedures voldoen aan de wettelijke vereisten zijn dezen geanalyseerd op basis van rechtsbronnen- en literatuuronderzoek. Gekeken is naar wat de wet voorschrijft en in hoeverre de gemeentelijke procedures hieraan voldoen.

Met betrekking tot bronnen anders dan de wet- en regelgeving, het gemeentelijke beleid en de gemeentelijke procedures is gekeken naar hun betrouwbaarheid. Om deze vast te stellen is gekeken naar de volgende criteria:

Ten eerste dient de bron gepubliceerd te zijn op een betrouwbare website of door een ander betrouwbaar medium. Afhankelijk van het soort bron kan hierbij gedacht worden aan een landelijk dagblad of de site daarvan, een (digitale) publicatie in een vakblad, een website of andere publicatie van een gezaghebbend orgaan zoals de Vereniging voor Nederlandse Gemeenten of een site van de Rijksoverheid.

Ten tweede dient de auteur van de bron betrouwbaar en/of gezaghebbend te zijn. Bij een juridische bron is het vooral relevant dat de auteur gezaghebbend of gespecialiseerd is op het rechtsgebied waarover hij of zij schrijft. Bij een niet-juridische bron is vooral de betrouwbaarheid van de auteur relevant.

Ten aanzien van de wet- en regelgeving zijn de artikelen eerst grondig gelezen en geïnventariseerd. Op deze manier is het niet alleen duidelijk wat de artikelen precies inhouden, maar ook hoe de artikelen zich tot elkaar verhouden. Daarnaast is de memorie van toelichting gebruikt om de bedoeling van de wetgever te doorgronden.

Met betrekking tot de relevante wetgeving is gezocht naar relevante artikelen die voldoen aan de hierboven genoemde criteria. Dezen zijn vervolgens gerangschikt op relevantie. Bronnen die voldoen aan de hierboven genoemde criteria en die voldoende relevant worden geacht zijn gelezen, waarna de kerninformatie hieruit geordend is.

Deze stappen zijn per deelvraag doorlopen. Met behulp van de informatie uit wet- en regelgeving en gemeentelijk beleid, in combinatie met de informatie uit andere bronnen, zoals boeken en artikelen in tijdschriften, zijn de deelvragen beantwoord. De antwoorden op de deelvragen hebben geresulteerd in het antwoord op de centrale vraag.

§1.4 Leeswijzer

Het inhoudelijke gedeelte van het onderzoek begint in hoofdstuk twee. In dat hoofdstuk zal het wettelijk kader, zowel op nationaal als internationaal niveau, uiteengezet worden. Hiervoor zal niet alleen gekeken worden naar hetgeen geregeld is in de huidige wetgeving, maar ook hoe de wetshistorie omtrent dit onderwerp eruit ziet en welke veranderingen in de toekomst mogelijk doorgevoerd zullen worden. Aangezien het juridisch kader bekend moet zijn voor er overgegaan kan worden tot analyse van de huidige situatie biedt dit hoofdstuk de basis voor de rest van het onderzoek.
Hierop volgend zal in hoofdstuk drie gekeken worden naar de huidige situatie bij de gemeenten Schijndel, Sint-Oedenrode en Veghel met betrekking tot het onderwerp. Dit hoofdstuk is fundamenteel om het contrast tussen de huidige situatie en de wenselijke situatie te tonen.
Vervolgens zal in hoofdstuk vier gekeken worden naar de daadwerkelijke uitvoering van dit beleid in de gemeenten Schijndel, Sint-Oedenrode en Veghel. Een goed beleid is namelijk volstrekt ineffectief als het niet wordt uitgevoerd.
Tot slot zullen in hoofdstuk vijf conclusies uit de in voorgaande hoofdstukken verzamelde gegevens volgen. Deze conclusies zullen vervolgens samengevoegd worden om de centrale vraag te kunnen beantwoorden. Hierna zullen enkele aanbevelingen worden gedaan over hoe de situatie in de onderzochte gemeenten, indien nodig, verbeterd kan worden en hoe deze aanbevelingen het best uitgevoerd kunnen worden.

Hoofdstuk 2: Wet- en Regelgeving

In dit hoofdstuk zal gekeken worden naar de geldende wet- en regelgeving omtrent datalekken. Voordat er gekeken kan worden naar het beleid van de drie te fuseren gemeenten is het immers van belang om te weten aan welke vereisten dit beleid moet voldoen. Hoewel dit onderzoek vooral aandacht besteedt aan de nieuwe wetgeving omtrent de meldplicht van datalekken zal in dit hoofdstuk ook gekeken worden naar de totstandkoming van deze meldplicht en naar toekomstige ontwikkelingen op dit gebied.

In dit hoofdstuk zal de volgende deelvraag worden beantwoord: *'Welke wettelijke vereisten gelden er met betrekking tot datalekken voor gemeenten op grond van de Wet Meldplicht Datalekken, de overige relevante nationale en Europese wet- en regelgeving en de bijbehorende jurisprudentie?'*

In dit hoofdstuk zal uitgebreid ingegaan worden op de vereisten omtrent de meldplicht van datalekken als genoemd in de Wet Bescherming Persoonsgegevens. Daarnaast zal worden ingegaan op een aantal relevante documenten hieromtrent, waaronder de memorie van toelichting en de Beleidsregels Meldplicht Datalekken. Hiervoor zal eerst gekeken worden naar de geschiedenis van de Wet Bescherming Persoonsgegevens en de gebeurtenissen die hebben geleid tot de totstandkoming van de Wet Meldplicht Datalekken. Ten slotte zal gekeken worden naar toekomstige ontwikkelingen op het gebied van wetgeving die mogelijk van invloed kunnen zijn op de Wet Meldplicht Datalekken.

Aangezien deze deelvraag betrekking heeft op de wettelijke vereisten omtrent datalekken en data-beveiliging is gekozen voor de onderzoeksmethode 'rechtsbronnen- en literatuuronderzoek'. Deze onderzoeksmethode is de enige logische keuze voor een deelvraag die in gaat op de inhoud van een wet. Op de rechtsbronnen en de bijbehorende documenten die voor de beantwoording van deze deelvraag geraadpleegd zullen worden zal een inhoudsanalyse worden toegepast. Dit is de namelijk de meest logische keuze wanneer een geschreven tekst bestudeert wordt. De Wet Meldplicht Datalekken zal de belangrijkste rechtsbron zijn, omdat voor de beantwoording van deze deelvraag gekeken zal worden naar de vereisten die hierin beschreven zijn. Daarnaast zal in mindere mate gebruik gemaakt worden van literatuur die betrekking hebben op dit onderwerp, andere wetgeving omtrent dit onderwerp en eventuele jurisprudentie die voor dit onderwerp relevant is.

De antwoorden die voortkomen uit dit hoofdstuk zullen in latere hoofdstukken de basis vormen voor het beantwoorden van deelvragen omtrent het beleid van de te fuseren gemeenten.

§2.1 Wetshistorie

Allereerst zal gekeken worden naar de chronologie van nationale en internationale wetten met betrekking tot bescherming van persoonsgegevens voor de invoering van de Wet Bescherming Persoonsgegevens in het jaar 2001. In deze paragraaf zal vooral gekeken worden naar wat deze wet- en regelgevingen zeggen over databeveiliging en datalekken.

§2.1.1 Europese wet- en regelgeving

In 1950 heeft de Raad van Europa het Europese Verdrag ter bescherming van de Rechten van de Mens opgesteld in navolging van het Internationale Verdrag ter bescherming van de Rechten van de Mens. In dit verdrag zijn een groot aantal rechten opgenomen voor inwoners van landen die het verdrag hebben geratificeerd. Nederland is een van de landen die dit verdrag heeft geratificeerd. In artikel 8 van dit verdrag is geregeld dat eenieder recht heeft op eerbiediging van privé-, familie- en gezinsleven[1]. Hierin staat ook dat '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[2]'. Samengevat houdt dit in dat de lidstaat hier enkel een inbreuk op kan maken door een wet in formele zin, indien dit noodzakelijk is wegens een van de hierboven genoemde gronden. Het EVRM ziet weliswaar niet direct op de bescherming van persoonsgegevens maar ziet in plaats daarvan op het recht op privacy. Onder dit recht valt ook het recht op de bescherming van persoonsgegevens. De EVRM zegt op zichzelf niets over databeveiliging en datalekken, maar was nochtans cruciaal in het proces dat leidde tot de Wet Meldplicht Datalekken als eerste verdrag dat zag op bescherming van persoonsgegevens.

In het jaar 1995 heeft de Europese Unie Richtlijn 95/46/EG ingevoerd[3]. Deze richtlijn geeft de lidstaten van de Europese Unie een basis om hun eigen wet op te stellen met betrekking tot de bescherming van persoonsgegevens. Deze richtlijn moest binnen 3 jaar na zijn ondertekening op 24 oktober 1995 door de lidstaten omgezet worden in wet- en regelgeving[4]. In Nederland is dit de Wet Bescherming Persoonsgegevens geworden[5]. Op het gebied van gegevensbeveiliging is in het bijzonder artikel 17 van deze richtlijn van belang. In dit artikel staat dat de lidstaten dienen te bepalen dat persoonsgegevens, zowel organisatorisch als technisch, voldoende beveiligd moeten zijn tegen 'vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking'. Bovendien geeft dit artikel aan dat de lidstaten moeten bepalen dat instanties die persoonsgegevens verwerken een verwerker moeten kiezen die de beveiliging van de persoonsgegevens kan waarborgen. Ten slotte is het nog relevant om te melden

Figuur 1: Tijdlijn wetgeving

[1] Art. 8 EVRM
[2] Art. 8 lid 2 EVRM
[3] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens
[4] Artikel 32 lid 1 van de Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens
[5] Wet Bescherming Persoonsgegevens, preambule

dat in artikel 24 van deze richtlijn is opgenomen dat de lidstaten dienen te bepalen dat sancties mogelijk zijn indien niet wordt voldaan aan de vereisten in de op deze richtlijn gebaseerde nationale wetgeving.

In 2013 heeft de Europese Commissie 'Verordening (EU) nr. 611/2013' ingevoerd. Deze regeling is direct bindend voor alle lidstaten van de Europese Unie[6]. Op grond van artikel 288 van het Verdrag Betreffende de Werking van de Europese Unie is een dergelijke verordening rechtstreeks toepasbaar in alle lidstaten en kunnen de burgers zich hier dus rechtstreeks op beroepen. Hoewel deze regeling vrij summier is voert deze belangrijke verplichtingen omtrent databeveiliging en datalekken door. Zo bevat deze regeling een meldplicht wanneer een datalek voorkomt[7], maar ook een uitzondering voor voldoende beveiligde data[8]. De artikelen 3 en 4 van deze regeling hebben veel gemeen met artikel 34a van de Wet Meldplicht Datalekken. De Nederlandse Wet Meldplicht Datalekken komt dan ook naar alle waarschijnlijkheid voort uit deze regeling, hoewel dit niet blijkt uit de memorie van toelichting.

§2.1.2 Nederlandse wet- en regelgeving

Op 1 juli 1989, voor de invoering van de EU-richtlijn 95/46/EG, is in Nederland de Wet Persoonsregistraties ingevoerd. Deze wet is de voorloper van de huidige Wet Bescherming Persoonsgegevens[9]. Hoewel de Wet Persoonsregistratie is ingevoerd voordat de EU-richtlijn 95/46/EG is vastgesteld staan in deze wet een aantal regelingen die veel overeenkomsten vertonen met deze richtlijn. Op het gebied van databeveiliging is vooral artikel 8 relevant. Hierin staat vrijwel dezelfde tekst als in artikel 17 van de EU-richtlijn 95/46/EG. In artikel 9 van deze wet staat opgenomen dat, indien een verwerker onvoldoende voldoet aan hetgeen is geregeld in de wet, deze een schadevergoeding zal moeten betalen aan de persoon om wiens persoonsgegevens het gaat. Hieronder valt ook de eerder genoemde beveiligingsplicht. Het onvoldoende beveiligen van persoonsgegevens waardoor deze verloren kunnen gaan, aangetast kunnen worden of waar door onbevoegden kennis van genomen kan worden, gewijzigd kan worden of verstrekt kan worden kon onder deze wet dus tot gevolg hebben dat de verwerker een schadevergoeding moest betalen aan degene om wiens persoonsgegevens het ging.

§2.2 Wet Bescherming Persoonsgegevens

Na de invoering van de EU-richtlijn 95/46/EG is in Nederland op 1 september 1998 op basis van deze richtlijn de Wet Bescherming Persoonsgegevens ingevoerd[10]. Deze wet diende ter vervanging van de Wet Persoonsregistraties[11]. In deze paragraaf zullen eveneens de artikelen met betrekking tot databeveiliging in de Wet Bescherming Persoonsgegevens

[6] Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie
[7] Artikel 3 van de Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie
[8] Artikel 4 van de Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie
[9] Art. 81 Wbp
[10] Preambule Wbp
[11] Art. 81 Wbp

uiteengezet worden. Hiervoor zal uitgegaan worden van de wettekst zoals deze was voor de invoering van de Meldplicht Datalekken op 1 januari 2016.

§2.2.1 Databeveiliging

Met betrekking tot beveiliging van persoonsgegevens is artikel 8 van de Wet Persoonsregistraties grotendeels overgenomen in artikel 13 van de Wet Bescherming Persoonsgegevens. Opvallend hierin is dat, hoewel de inhoud van de twee artikelen vrijwel gelijk is, de variant die is opgenomen in de Wet Bescherming Persoonsgegevens minder uitgebreid lijkt te zijn. In dit artikel staat dat technische en organisatorische maatregelen getroffen dienen te worden tegen 'verlies of tegen enige vorm van onrechtmatige verwerking[12]', dit in tegenstelling tot de uitgebreidere beschrijving die was opgenomen in de Wet Persoonsregistraties. Uit de memorie van toelichting blijkt dat de term 'enige vorm van onrechtmatige verwerking' gelijk staat aan 'de aantasting van de gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan[13]'. Dit is vrijwel identiek aan de term die gebruikt wordt in Richtlijn 95/46/EG en de Wet Persoonsregistraties.

Een belangrijk aspect van dit wetsartikel is de zinssnede 'passende technische en organisatorische maatregelen[14]'. Volgens de wettekst moeten de maatregelen een passend beveiligingsniveau garanderen, gelet op de risico's van de verwerking en de aard van de te beschermen gegevens. Hierin dient ook rekening gehouden te worden met de 'stand van de techniek en de kosten van de tenuitvoerlegging[15]'. Uit de memorie van toelichting blijkt dat de term 'passend' tweeledig uitgelegd dient te worden. Enerzijds duidt de term 'passend' op het feit dat deze maatregelen in overeenstemming moeten zijn met de stand van de techniek. Volgens de memorie van toelichting is dit niet verder uitgewerkt omdat de wettekst dan in hoge mate tijdgebonden zou zijn, waardoor deze in korte tijd verouderd zou zijn. Anderzijds duidt de term 'passend' op het feit dat de mate van beveiliging proportioneel moet zijn aan de gevoeligheid van de te verwerken persoonsgegevens of de grootte van de consequenties die het verlies of enige vorm van onrechtmatige verwerking van deze persoonsgegevens tot gevolg heeft. In essentie houdt dit in dat verantwoordelijken niet altijd de zwaarst mogelijke beveiliging moeten toepassen om de persoonsgegevens te beschermen, omdat dit in veel gevallen redelijkerwijs niet haalbaar noch noodzakelijk is.

Artikel 14 van deze wet ziet erop toe dat de verantwoordelijke, zijnde degene die de gegevens zou verwerken, er zorg voor moet dragen dat er voldoende technische en organisatorische maatregelen getroffen dienen te worden tegen 'verlies of tegen enige vorm van onrechtmatige verwerking', ook indien de verwerking van persoonsgegevens aan een derde wordt overgedragen. In dit geval moet eveneens voldaan worden aan de hierboven genoemde vereisten. Indien hier niet of onvoldoende aan wordt voldaan is de verantwoordelijke aansprakelijk voor alle schade die betrokkenen leiden door een gebrek aan voldoende passende beveiligingsmaatregelen, waaronder data die gelekt wordt.

In artikel 50 van de Wet Bescherming Persoonsgegevens staat dat indien de verantwoordelijke of de bewerker handelt in strijd met 'het bij of krachtens deze wet

[12] Art. 13 Wbp
[13] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 98
[14] Art. 13 Wbp
[15] Art. 13 Wbp

bepaalde', waardoor de betrokkene schade leidt of dreigt te leiden, de rechter kan bepalen dat de verantwoordelijke of de verwerker dit gedrag moet staken en dat deze maatregelen moet treffen tot het herstel van de gevolgen van dat gedrag. Onder de term 'het bij of krachtens deze wet bepaalde' vallen uiteraard ook de hierboven genoemde artikelen uit de Wet Bescherming Persoonsgegevens. Op grond van artikel 49 van deze wet kan de betrokkene ook schadevergoeding ontvangen voor gedragingen in strijd met het 'bij of krachtens deze wet bepaalde'. Indien de schade geheel of gedeeltelijk uit immateriële schade bestaat wordt een schadevergoeding naar billijkheid toegewezen[16]. Deze twee artikelen dienen hetzelfde doel als de artikelen 9 en 10 in de wet Persoonsregistraties. De zwaarte van de risicoaansprakelijkheid is echter, in overeenstemming met Richtlijn 95/46/EG afgezwakt[17].

De artikelen 62 tot en met 64 van de Wet Bescherming Persoonsgegevens geven verantwoordelijke organisaties de mogelijkheid om een functionaris gegevensbescherming te benoemen. Deze functionaris ziet toe op alle verwerking van persoonsgegevens door de verantwoordelijke die hem heeft benoemd en door de andere verantwoordelijken in de organisatie die zijn aangesloten bij de organisatie die hem heeft benoemd[18]. Deze functionaris kan aanbevelingen doen aan de verantwoordelijken die strekken tot een betere bescherming van de gegevens die worden verwerkt[19].

Op grond van artikel 65 kan het College Bescherming Persoonsgegevens bestuursdwang opleggen aan verantwoordelijken die niet voldoen aan het in deze wet gestelde verplichtingen. Een last onder bestuursdwang, zoals geregeld in artikel 5:21 van de Algemene Wet Bestuursrecht, geeft de Autoriteit Persoonsgegevens de mogelijkheid om de verantwoordelijke te verplichten om de onwenselijke situatie te herstellen en, indien zij dit niet doen, om de last door zelfstandig handelen ten uitvoer te brengen. Uit de jurisprudentie blijkt echter niet dat hier vaak gebruik van wordt gemaakt. Op grond van artikel 5:32 lid 1 van de Algemene Wet Bestuursrecht kan in plaats van een last onder bestuursdwang ook een last onder dwangsom worden opgelegd.

§2.3 Wet Meldplicht Datalekken

In deze paragraaf zal de Wet Meldplicht Datalekken uiteengezet worden. Allereerst zal besproken worden hoe de Wet Meldplicht Datalekken tot stand is gekomen. Daarna zullen de veranderingen in de Wet Bescherming Persoonsgegevens omschreven worden, evenals hetgeen dat is geregeld in de bijbehorende Beleidsregels Meldplicht Datalekken.

§2.3.1 Ontstaan van de Meldplicht Datalekken

De Meldplicht Datalekken is ingevoerd op 1 januari 2016 naar aanleiding van een groot aantal incidenten waarbij door een inbreuk op de beveiliging van, onder meer, websites veel persoonsgegevens openbaar werden, wat betrokkenen ernstige schade opleverde[20]. Een veelbesproken voorbeeld van een dergelijk incident is de website Ashley Madison. Op deze website konden getrouwde mannen op zoek naar een 'scharrel'. Toen hackers deze

[16] Art. 49 lid 2 Wbp
[17] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 176
[18] Art. 64 lid 1 Wbp
[19] Art. 64 lid 4 Wbp
[20] *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 1

gegevens buit maakten en vervolgens in de openbaarheid brachten, werden de namen van alle mannen op deze site bekend, wat tot veel ophef leidde.

Om die reden is een meldplicht bij datalekken, zelfs bij overheidsinstanties, al in het regeerakkoord van kabinet-Rutte I opgenomen[21]. De uitbreiding van de boetebevoegdheid in diezelfde Wet Meldplicht Datalekken is opgenomen in het regeerakkoord van kabinet-Rutte II[22]. Door middel van deze boete wil de regering het College Bescherming Persoonsgegevens, welke vanaf 1 januari 2016 is omgedoopt tot de Autoriteit Persoonsgegevens, meer mogelijkheden bieden om datalekken tegen te gaan.

§2.3.2 Definitie van een Datalek

Alvorens er kan worden gekeken naar de vraag wat de gemeente moet doen indien er sprake is van een datalek en hoe ze dergelijke datalekken kunnen voorkomen dient eerst gekeken te worden naar de definitie van een datalek.

Hoewel de term ‘datalek’ in de naam van de wetswijziging zit, en in het dagelijks spraakgebruik ook vaak wordt gebruikt, staat deze term niet als zodanig in de wet. Artikel 34a van de Wet Bescherming Persoonsgegevens, het artikel dat de meldplicht introduceert, spreekt van een ‘inbreuk op de beveiliging, bedoeld in artikel 13’. Artikel 13 van de Wet Bescherming persoonsgegevens spreekt van ‘*verlies of […] enige vorm van onrechtmatige verwerking*’[23]. Een datalek, zoals genoemd in de naam van deze wetswijziging is dus een inbreuk op de beveiliging van digitale bestanden, in de vorm van technische en organisatorische maatregelen, welke dienen te beschermen tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens.

De term ‘datalek’ als genoemd in de Wet Meldplicht Datalekken is technisch gezien incorrect, aangezien de wet klaarblijkelijk betrekking heeft op inbreuk op de beveiliging tegen verlies of enige vorm van onrechtmatige verwerking. Om verwarring te voorkomen die mogelijk zou voortkomen uit het plotseling veranderen van de gebruikte term zal in het vervolg de term ‘datalek’ gebruikt blijven worden. Wanneer deze term in dit rapport gebruikt wordt, wordt hiermee een inbreuk bedoeld worden zoals besproken in deze paragraaf.

§2.3.3 Meldplicht aan de Autoriteit Persoonsgegevens

De Meldplicht Datalekken geldt echter niet voor alle datalekken. Er zijn enkele vereisten waar een datalek aan moet voldoen voordat deze gemeld dient te worden aan de Autoriteit Persoonsgegevens. Deze vereisten, die veelal zijn opgenomen in artikel 34a van de Wet Bescherming Persoonsgegevens en de memorie van toelichting van de wetswijziging, zullen in deze paragraaf worden besproken.

Op grond van artikel 34a lid 1 van de Wet Bescherming Persoonsgegevens dient het datalek te leiden tot ‘ernstige nadelige gevolgen […] voor de bescherming van persoonsgegevens’ of de aanzienlijke kans hiertoe. Op grond van de memorie van toelichting van de Wet Meldplicht Datalekken dienen er ruwweg twee stappen te worden ondernomen voordat

[21] *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 2
[22] *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 2
[23] De inhoud van deze term is reeds in paragraaf 2.2.1 besproken

bepaald kan worden of er sprake is van ernstige nadelige gevolgen voor de bescherming van persoonsgegevens[24].

Allereerst dient gekeken te worden of er sprake is van mogelijke nadelige gevolgen in de vorm van verlies of onrechtmatige verwerking van persoonsgegevens. Op grond van de memorie van toelichting moet dit zo objectief mogelijk bepaald worden en dient daarbij gekeken te worden naar de feiten en omstandigheden. De aanmerkelijke kans dat de persoonsgegevens worden blootgesteld aan verlies of onrechtmatige verwerking dient redelijkerwijs aanwezig te zijn. Met betrekking tot de hiervoor genoemde aanmerkelijke kans moet gekeken worden naar de concrete feiten en omstandigheden. Niet alleen dient er gekeken te worden naar hoe groot het risico op een inbreuk is, maar ook wat de consequenties zijn indien deze data daadwerkelijk gelekt worden.

Ten tweede dient gekeken te worden naar de vraag of een dergelijke inbreuk leidt tot nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkene. Hierbij spelen vooral aard en omvang van de onrechtmatige verwerking een grote rol. Indien bijvoorbeeld bankgegevens gelekt worden is het risico op nadelige gevolgen voor de persoonlijke levenssfeer van betrokkene vele malen groter dan wanneer bijvoorbeeld gegevens van een sportclub gelekt worden.

Indien zowel het risico van de inbreuk, de kans op de inbreuk en de consequenties van de inbreuk groot genoeg zijn dient een datalek gemeld te worden.

In de Beleidsregels Meldplicht Datalekken van de Autoriteit Persoonsgegevens, welke invulling geven aan de inhoud van artikel 34a van de Wet Bescherming Persoonsgegevens, is opgenomen dat bij het lekken van persoonsgegevens van gevoelige aard een melding over het algemeen noodzakelijk is. Volgens de beleidsregels is hiervan in ieder geval sprake bij: bijzondere persoonsgegevens als genoemd in artikel 16 van de Wet Bescherming Persoonsgegevens, gegevens over de financiële of economische situatie van de betrokkene, gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, zoals informatie over een gokverslaving, relatieproblemen etc., inloggegevens en gegevens die kunnen worden misbruikt voor (identiteits)fraude.

Naast de standaard meldplicht van datalekken is het ook relevant om aan te geven hoe de verhouding tussen verantwoordelijken en verwerkers eruit ziet. Zoals in paragraaf 2.2.1 reeds is beschreven is de verantwoordelijke, op grond van artikel 14 lid 3 sub b van de Wet Bescherming Persoonsgegevens, verantwoordelijk voor de beveiliging van de persoonsgegevens die de verwerker namens de verantwoordelijke verwerkt. Indien er een datalek ontstaat is de verantwoordelijke verantwoordelijk voor het melden van dit datalek op grond van artikel 14 lid 3 sub c van de Wet Bescherming Persoonsgegevens.

§2.3.4 Meldplicht aan betrokkene(n)

Op grond van artikel 34a lid 2 van de Wet Bescherming Persoonsgegevens dient de verantwoordelijke in bepaalde gevallen het datalek ook te melden aan de betrokkene(n). Hier is in essentie maar één vereiste voor, die hieronder uiteen gezet zullen worden.

[24] *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 7

Op grond van artikel 34a lid 2 van de Wet Bescherming Persoonsgegevens dient de betrokkene in kennis gesteld te worden van een datalek 'indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer'. Om te bepalen of dit het geval is dient wederom gekeken te worden naar de omvang en de consequenties van het verlies of de onrechtmatige verwerking. Indien de verantwoordelijke van mening is dat het datalek nadelige gevolgen heeft of zal hebben voor de verwerking van persoonsgegevens, maar waarschijnlijk geen ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, kan de Autoriteit Persoonsgegevens, indien zij het niet eens is met deze inschatting, op grond van lid 7 van dit artikel alsnog vorderen dat de betrokkene geïnformeerd wordt.

Een melding op grond van artikel 34a lid 2 van de Wet Bescherming persoonsgegevens is echter op grond van lid 6 van ditzelfde artikel niet noodzakelijk indien de gegevens versleuteld zijn waardoor deze onbegrijpelijk of ontoegankelijk zijn voor personen die geen recht hebben om van deze persoonsgegevens kennis te nemen. Hierbij wordt gekeken naar de huidige stand van de technologie.

Zelfs wanneer het datalek gemeld wordt aan de betrokkene betekent dit niet dat de verantwoordelijke niet langer verantwoordelijk is voor enige schade die de betrokkene lijdt ten gevolge van het verlies of de onrechtmatige verwerking van zijn of haar persoonsgegevens[25]. Wanneer het datalek echter wordt gemeld aan de betrokkene voldoet de verantwoordelijke aan zijn verplichting tot schadebeperking. Dit houdt in dat de verantwoordelijke zich in bepaalde situaties kan beroepen op de eigen schuld van de betrokkene, indien deze heeft nagelaten om voorzorgsmaatregelen te treffen nadat het datalek aan hem is gemeld.

Op grond van artikel 6:162 van het Burgerlijk Wetboek kan de betrokkene, indien er sprake is van een datalek die de verantwoordelijke had kunnen voorkomen, een schadevergoeding eisen van de verantwoordelijke op grond van de onrechtmatige daad. De onrechtmatige daad in kwestie zal, bij het verzaken van de meldplicht, waarschijnlijk een nalaten in strijd met een wettelijke plicht zijn, als genoemd in artikel 6:162 lid 2 van het Burgerlijk Wetboek.

2.3.5 Inhoud melding

Op grond van de Wet Meldplicht Datalekken dient een melding aan de Autoriteit Persoonsgegevens en eventueel aan een betrokkene te voldoen aan een aantal vereisten. Deze vereisten zullen hieronder uiteengezet en waar nodig uitgelegd worden.

Ten eerste dient, op grond van artikel 34a lid 3 van de Wet Meldplicht Datalekken de kennisgeving aan de Autoriteit Persoonsgegevens en de (eventuele) betrokkene in ieder geval de volgende zaken te bevatten: 'de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken'. De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken zijn vooral relevant voor de betrokkenen. Indien de betrokkene deze maatregelen niet overneemt kan er mogelijk sprake zijn van eigen schuld, zoals besproken in de vorige paragraaf.

[25] *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 9

Ten tweede dient de kennisgeving aan het college op grond van artikel 34a lid 4 van de Wet Meldplicht Datalekken eveneens de volgende zaken te bevatten: ‘een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen’. Aangezien de verantwoordelijke dergelijke maatregelen moet melden dient, voor het melden van deze datalekken, onderzoek gedaan te worden naar manieren om een dergelijk datalek in de toekomst tegen te gaan.

Ten derde dient de kennisgeving op grond van artikel 34a lid 5 van de Wet Meldplicht Datalekken een behoorlijke en zorgvuldige informatievoorziening, het voorzien van informatie aan belanghebbenden, te waarborgen. Hierbij dient rekening gehouden te worden met de aard van de inbreuk, de gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging.

Ten slotte kunnen op grond van artikel 34a lid 11 van de Wet Bescherming Persoonsgegevens bij algemene maatregel van bestuur nadere regels worden gesteld met betrekking tot de kennisgeving. Hoewel er geen algemene maatregel van bestuur is opgesteld is door middel van de Beleidsregels Meldplicht Datalekken de procedure wel verduidelijkt. In de bijlage van deze beleidsregels is een vragenlijst opgenomen van informatie die in een melding dient te worden opgenomen[26]. Deze vragenlijst is gebaseerd op bijlage I van de Europese Verordening 611/2013. Deze vragenlijst is opgedeeld in enkele categorieën zijnde: aard van de melding, wettelijk kader van de melding, algemene informatie en contactgegevens, gegevens over het datalek, vervolgacties naar aanleiding van het datalek, inlichten van de betrokkene, technische beschermingsmaatregelen, internationale aspecten en vervolgmelding.

§2.3.6 Boetebevoegdheid

Naast de meldplicht bij datalekken is er nog een andere grote verandering doorgevoerd in de Wet Bescherming Persoonsgegevens. De boetebevoegdheid die de Autoriteit Persoonsgegevens heeft wordt namelijk bij deze wetswijziging uitgebreid. Waar aanvankelijk slechts voor een beperkt aantal overtredingen een relatief lage boete kon worden opgelegd is zowel het aantal beboetbare overtredingen als de hoogte van de eventuele boete verhoogd.

Op grond van artikel 66 lid 1 van de Wet Bescherming Persoonsgegevens juncto artikel 23 lid 4 van het Wetboek van Strafrecht kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen van maximaal 20.250 euro bij twee mogelijke overtredingen. Allereerst is een dergelijke boete mogelijk bij de verwerking van persoonsgegevens door een rechtspersoon die geen vestiging heeft in de Europese unie, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt overeenkomstig de bepalingen van deze wet[27]. Ten tweede is een dergelijke boete mogelijk bij de doorgifte van persoonsgegevens naar een land buiten de Europese Unie, indien dit door de Minister van Justitie bij ministeriële regeling of bij besluit is verboden naar aanleiding van een besluit van de Commissie van de Europese Gemeenschappen of de Raad van de Europese Unie[28].

[26] Beleidsregels voor toepassing van artikel 34a van de Wbp, p. 52-55
[27] Art. 4 lid 3 en lid 2 Wbp
[28] Art. 78 lid 2 aanhef en sub a Wbp

Op grond van artikel 66 lid 2 van de Wet Bescherming Persoonsgegevens juncto artikel 23 lid 4 van het Wetboek van Strafrecht kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen van maximaal 820.000 euro voor een groot aantal verschillende overtredingen. Op het gebied van databeveiliging en datalekken zijn de overtredingen als genoemd in de artikelen 13, zijnde de beveiligingsplicht en 34a, zijnde de meldplicht het belangrijkste. Indien de data niet voldoende beveiligd zijn of van een datalek waarbij melding verplicht is geen melding wordt gemaakt, kan een gemeente onder andere een dergelijke boete opgelegd krijgen. Een boete kan in beginsel enkel opgelegd worden nadat de Autoriteit Persoonsgegevens een bindende aanwijzing heeft opgelegd op grond van artikel 66 lid 3 van de Wet Bescherming Persoonsgegevens. Indien de verantwoordelijke niet binnen de hiervoor gestelde periode voldoet aan deze bindende aanwijzing kan de Autoriteit Persoonsgegevens alsnog een bestuurlijke boete opleggen. Een dergelijke bindende aanwijzing is niet noodzakelijk indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid. Onder ernstig verwijtbare nalatigheid wordt verstaan: 'grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen'[29].

§2.4 Toekomstige wetgeving

Hoewel de Wet Bescherming Persoonsgegevens en de bijbehorende Meldplicht Datalekken op dit moment in Nederland geldig zijn zal dit niet altijd het geval zijn. Nieuwe wetgeving, nationaal of internationaal, kan de huidige wetgeving irrelevant of ongeldig maken. In deze paragraaf zal gekeken worden naar de directe toekomst op het gebied van Bescherming van Persoonsgegevens en Meldplicht Datalekken.

§2.4.1 Europese Algemene Verordening Gegevensbescherming

Sinds het jaar 2012 is de Europese Commissie bezig met het opstellen van een Europese Algemene Verordening Gegevensbescherming[30]. Hoewel deze verordening nog niet is aangenomen is deze al wel goedgekeurd door het Europees parlement op 12 maart 2014 en door de Raad op 15 juni 2015[31]. Er wordt verwacht dat deze in de loop van het jaar, onder Nederlands EU-voorzitterschap, vastgesteld zal worden[32]. Deze verordening zal Richtlijn 95/46/EG vervangen, waardoor ook de hierop gebaseerde Wet Bescherming Persoonsgegevens vervangen zal worden.

Hoewel de exacte wettekst nog niet officieel is mag aangenomen worden dat de uiteindelijke versie veel zal lijken op de meest recente conceptversie. Hieruit kan gedeeltelijk worden afgeleid hoeveel de wet werkelijk zal veranderen. De relevante artikelen zullen kort uitgelegd worden en er zal aangegeven worden wat de grootste veranderingen zijn. Op het gebied van databeveiliging en Meldplicht Datalekken zijn de volgende artikelen relevant.

Artikel 30 van de Europese Algemene Verordening Gegevensbescherming ziet op de beveiliging van data. Lid 1 van dit artikel is praktisch gelijk aan artikel 13 van de Wet Bescherming Persoonsgegevens. De leden 3, 4 en 5 van dit artikel geven de Europese

[29] Beleidsregels voor toepassing van artikel 34a van de Wbp, p. 50
[30] Commissiedocument nr. 11 van 2012
[31] Van Geenen 2015.
[32] Van Geenen 2015

Commissie additionele opties om te zorgen dat deze beveiliging ook daadwerkelijk plaatsvindt.

De artikelen 31 en 32 van de Europese Algemene Verordening Gegevensbescherming ziet op de Meldplicht Datalekken. Deze artikelen hebben veel gemeen artikel 34a van de Wet Bescherming Persoonsgegevens. Een belangrijk verschil is dat in dit artikel, in plaats van voor de algemene term ‘onverwijld’, is gekozen voor een periode van 24 uur. Het is mogelijk om de melding later te doen, maar dat moet voldoende gemotiveerd worden.

Ten slotte is het nog relevant om aan te geven dat de Autoriteit Persoonsgegevens hoogstwaarschijnlijk zal blijven bestaan. Op grond van artikel 46 van de Europese Algemene Verordening Gegevensbescherming dient iedere lidstaat een ‘toezichthoudende autoriteit’ in te stellen. Het lijkt zeer waarschijnlijk dat deze rol de Autoriteit Persoonsgegevens ten deel valt, waardoor zij het grootste deel van hun bevoegdheden behouden.

Hoofdstuk 3: Huidig beleid

In dit hoofdstuk zal gekeken worden naar het beleid en de protocollen van de drie te fuseren gemeenten; Schijndel, Sint-Oedenrode en Veghel. Er zal specifiek gekeken worden naar het beleid en de protocollen van de drie gemeenten op het gebied van databeveiliging en datalekken.

In dit hoofdstuk zal de volgende deelvraag worden beantwoord: *'Door middel van welke protocollen en processen worden de wettelijke regels met betrekking tot datalekken binnen de drie te fuseren gemeenten uitgevoerd en wat houden deze protocollen en processen in?'.*

In dit hoofdstuk zal worden ingegaan op de processen en protocollen van de drie te fuseren gemeenten op het gebied van databeveiliging, datalekken en de meldplicht daarvan. De hoofdpunten hiervan zullen worden beschreven. Op het gebied van de Wet Meldplicht Datalekken zijn er voor gemeenten in essentie twee zaken die goed geregeld dienen te worden: de beveiliging van de gegevens en wat er gebeurt als er een datalek plaatsvindt. Beide onderwerpen zullen per gemeente behandeld worden.

Aangezien deze deelvraag betrekking heeft op de huidige processen en protocollen die binnen de drie te fuseren gemeenten gelden zal voor deze deelvraag vooral gebruik gemaakt worden van de onderzoeksstrategie 'praktijkonderzoek'. Specifiek zal bij het beantwoorden van deze vraag sprake zijn van een 'kwalitatief praktijkonderzoek'. Binnen dit kwalitatief praktijkonderzoek zal de onderzoeksstrategie 'casestudy' de boventoon voeren, aangezien er gekeken wordt naar het huidige beleid en de huidige processen. Op het gebied van bronnen zal enerzijds gekeken worden naar de bronsoort 'documenten' en anderzijds naar de bronsoort 'personen'. Uit documenten moet immers afgeleid worden hoe het huidige beleid en de huidige processen en protocollen eruit zien, waarna personen, zoals beveiligingsfunctionarissen, uiteen kunnen zetten hoe dit in de praktijk in zijn werk gaat. Voor de documenten zal een inhoudsanalyse worden toegepast, voor de personen een interview.

De informatie die in dit hoofdstuk gegeven wordt zal in het volgende hoofdstuk de basis vormen voor het beantwoorden van de derde deelvraag.

§3.1 Baseline Informatiebeveiliging Gemeenten

Binnen alle drie de te fuseren gemeenten is het databeveiligingsbeleid gebaseerd op de strategische Baseline Informatiebeveiliging Gemeenten (hierna: BIG) en de tactische BIG van de Informatie Beveiligingsdienst Gemeenten (hierna: IBD). De IBD is een initiatief van het Kwaliteitsinstituut Nederlandse Gemeenten (hierna: KING) en de Vereniging Nederlandse Gemeenten (hierna: VNG). De strategische en tactische BIG van de IBD zijn twee documenten die voor gemeenten zijn opgesteld om hun informatiebeveiliging te regelen en te toetsen[33]. Deze documenten zijn gebaseerd op de internationale standaarden voor informatiebeveiliging: NEN/ISO 27002:2007 en de BIR[34]. De strategische BIG is een raamwerk waar de elementen van databeveiliging aan gehangen kunnen worden. De tactische BIG is een verdieping hierop en bevat een groot aantal maatregelen die genomen kunnen worden met betrekking tot databeveiliging. In de volgende paragraaf zal de

[33] 'Strategische en Tactische BIG', www.ibdgemeenten.nl/producten/strategische-en-tactische-big/
[34] 'Strategische en Tactische BIG', www.ibdgemeenten.nl/producten/strategische-en-tactische-big/

algemene versie van de tactische BIG besproken worden. De strategische BIG is per gemeente verschillend en zal dus in de volgende paragrafen per gemeente apart besproken worden.

§3.1.1 Algemene Tactische Baseline

De Tactische BIG van de IBD is een document dat voor gemeenten is opgesteld om hun informatiebeveiliging aan te toetsen[35].

De eerste vijf hoofdstukken van de Tactische BIG gaan in op de implementatie en uitvoering hiervan. Hierin wordt onder andere beschreven hoe de Tactische BIG tot stand is gekomen, hoe deze binnen een gemeente ingevoerd en onderhouden kan worden en hoe een risicoanalyse eruit kan zien.

De rest van de Tactische Baseline is opgesplitst in tien categorieën in evenveel hoofdstukken. Deze categorieën zijn:

- Organisatie van de informatiebeveiliging,
- Beheer van bedrijfsmiddelen,
- Personele beveiliging,
- Fysieke beveiliging en beveiliging van de omgeving,
- Beheer van Communicatie- en Bedieningsprocessen,
- Toegangsbeveiliging,
- Verwerving, ontwikkeling en onderhoud van informatiesystemen,
- Beheer van informatiebeveiligingsincidenten,
- Bedrijfscontinuïteitsbeheer,
- Naleving.

De categorie ‘Beheer van informatiebeveiligingsincidenten’ gaat vooral in op het melden van datalekken. De overige categorieën hebben betrekking op de databeveiliging.

De eerste categorie, Organisatie van de informatiebeveiliging, is opgedeeld in twee onderdelen. In het eerste onderdeel worden richtlijnen gegeven met betrekking tot de interne organisatie van databeveiliging. Een groot deel van de informatie in dit onderdeel staat eveneens vermeld in de hiervoor genoemde categorie informatiebeveiligingsbeleid. Belangrijke punten in dit onderdeel zijn dat het College van B&W de informatiebeveiligingsdoelstellingen waarborgt, dat de CISO de beveiliging coördineert en dat er een geheimhoudingsplicht moet zijn. In het tweede onderdeel worden richtlijnen gegeven met betrekking tot externe partijen en hun rol in databeveiliging. Kort samengevat: indien een externe partij wordt ingeschakeld dient er een risico-afweging plaats te vinden, waarop de beslissing om een externe partij in te huren wordt gebaseerd. Gebaseerd op deze risico-afweging dient vervolgens bepaald te worden welke toegang deze derde krijgt en hoe de betrokken gegevens beveiligd worden.

De tweede categorie, Beheer van bedrijfsmiddelen, is eveneens opgedeeld in twee onderdelen. In het eerste onderdeel worden zaken omtrent de verantwoordelijkheid voor bedrijfsmiddelen geregeld. Hierin staat hoofdzakelijk dat alle bedrijfsmiddelen geïnventariseerd dienen te worden, dat elk bedrijfsmiddel een verantwoordelijke dient te

[35] ‘Strategische en Tactische BIG’, www.ibdgemeenten.nl/producten/strategische-en-tactische-big/

hebben en dat bedrijfsmiddelen verantwoordelijk gebruikt dienen te worden. In het tweede onderdeel worden zaken omtrent de bescherming van informatie geregeld. Hierin staat voornamelijk dat er richtlijnen horen te zijn waarin staat hoe informatie geclassificeerd dient te worden.

De derde categorie, Personele Beveiliging, is opgedeeld in drie onderdelen. Deze categorie gaat over het informeren van personeel en over het zorgdragen dat het personeel zijn verantwoordelijkheden begrijpt en kan uitvoeren. De drie onderdelen in deze categorie omvatten de periode voorafgaand aan het dienstverband, de periode gedurende het dienstverband en de periode na het dienstverband. Vooraf dient ervoor gezorgd te worden dat in het arbeidscontract voldoende aandacht besteed wordt aan informatiebeveiliging en er dient een screening plaats te vinden ter verificatie van de achtergrond van de werknemer. Gedurende het dienstverband dient aandacht besteed te worden aan training van de werknemer op het gebied van informatiebeveiliging en het uitvoeren van disciplinaire maatregelen, indien noodzakelijk. Na het dienstverband dient de gemeente er zorg voor te dragen dat de ex-werknemer geen bedrijfsmiddelen meer in zijn bezit heeft en dat zijn toegang tot de informatiesystemen wordt geblokkeerd.

De vierde categorie, Fysieke beveiliging en beveiliging van de omgeving, is opgedeeld in twee onderdelen. Het eerste onderdeel gaat in op de beveiliging van ruimten in de gebouwen en van de omgeving. De omgeving en de gebouwen zijn opgedeeld in verschillende beveiligingszones die elk een bepaald beveiligingsniveau hebben. In essentie houdt dit in dat ruimtes met gevoeligere informatie beter beveiligd zijn dan ruimtes met minder gevoelige informatie. Onder zone 0 valt ‘de omgeving van het gebouw’. Onder zone 1 vallen ‘de wachtruimten en de spreekkamers’. Onder zone 2 vallen ‘de werkruimten’. Onder zone 3 vallen ‘de ICT-ruimte/beveiligde ruimte voor bijvoorbeeld paspoortopslag’. Omtrent het werken in veilige ruimten is opgenomen dat het maken van opnames in beveiligde ruimten niet is toegestaan zonder expliciete toestemming en dat een ruimte afgesloten hoort te zijn indien er zich geen personen bevinden. Ook hoort de ruimte regelmatig gecontroleerd te worden. Het tweede onderdeel gaat in op de beveiliging van apparatuur tegen diefstal, verlies, schade, etc.

De vijfde categorie, Beheer van Communicatie- en Bedieningsprocessen, is opgedeeld in tien onderdelen. Deze categorie gaat over de beveiliging van ICT-processen. Het eerste onderdeel gaat over het veilige gebruik van ICT-voorzieningen. Het tweede onderdeel gaat over exploitatie van deze ICT-voorzieningen door een derde partij en hoe de beveiliging in zijn werk gaat. Het derde onderdeel gaat over de beveiliging van het systeem tegen storingen door onder andere updates. Het vierde onderdeel gaat over de beveiliging van het systeem tegen virussen en het gebruik van ‘mobile code’, software die tussen computers wordt getransporteerd, op een veilige manier. Het vijfde onderdeel gaat over het maken, beveiligen en onderhouden van back-ups. Het zesde onderdeel gaat over netwerkbeveiliging tegen bedreigingen, zoals hackers. Het zevende onderdeel gaat over de behandeling van de media ter voorkoming van onder andere het onbevoegd openbaar maken van gegevens. Het achtste onderdeel gaat over de uitwisseling van informatie binnen de gemeente en hoe ervoor gezorgd moet worden dat dit op een veilige manier gebeurt. Het negende onderdeel gaat over de bewerkstelligen van de beveiliging van diensten voor e-commerce en het veilig gebruik hiervan. Het tiende onderdeel gaat over de controle met betrekking tot onbevoegde informatieverwerking.

De zesde categorie, Toegangsbeveiliging, is opgedeeld in zeven onderdelen. Het eerste onderdeel geeft aan dat de toegang tot informatie beheerst moet worden door middel van, onder andere, het opstellen van een toegangsbeleid. Het tweede onderdeel geeft aan dat toegangsrechten van gebruikers tot de informatiesystemen goed geregeld dienen te worden en dat onbevoegde toegang voorkomen moet worden. Het derde onderdeel geeft aan dat gebruikers onbevoegde toegang tot informatiesystemen moeten voorkomen door het kiezen van een wachtwoord dat sterk genoeg is en het voldoen aan een 'clean desk- en clear screen-beleid'. Het vierde onderdeel geeft aan dat toegang tot netwerken gereguleerd moet worden en dat moet worden voorkomen dat onbevoegden toegang krijgen tot de netwerken. Het vijfde onderdeel geeft aan dat onbevoegde toegang tot besturingssystemen voorkomen dient te worden door middel van beveiligde inlogprocedures, gebruikersidentificatie en -authenticatie, en wachtwoordbeheer. Het zesde onderdeel geeft aan dat onbevoegde toegang tot informatie in toepassingssystemen voorkomen dient te worden door middel van het beperken van toegang tot deze informatie voor personeel waarvoor het niet relevant is en door middel van het isoleren van gevoelige gegevens. Het zevende onderdeel geeft aan dat er formeel beleid moet zijn met betrekking tot draagbare computers en telewerken om het risico op dataverlies te minimaliseren.

De zevende categorie, Verwerving, ontwikkeling en onderhoud van informatiesystemen, heeft betrekking op de beveiliging en het beheer van informatiesystemen. Deze categorie is opgedeeld in zes onderdelen. Het eerste onderdeel geeft aan dat beveiliging een integraal deel dient uit te maken van informatiesystemen. Het tweede onderdeel geeft aan dat informatie binnen systemen op een correcte manier verwerkt dient te worden. Het derde onderdeel geeft aan dat de vertrouwelijkheid, authenticiteit en integriteit van informatie gewaarborgd dient te worden door middel van cryptografische beheersmaatregelen. Het vierde onderdeel geeft aan dat systeembestanden beveiligt dienen te worden door middel van toegangsbeheersing. Het vijfde onderdeel geeft aan dat de beveiliging van toepassingsprogrammatuur- en informatie gehandhaafd dient te worden. Het zesde onderdeel geeft aan dat risico's moeten worden gemitigeerd door technische kwetsbaarheden, die door publicatie bekend zijn geworden, te herstellen.

De achtste categorie, Beheer van Informatiebeveiligingsincidenten, gaat over hoe een informatiebeveiligingsincident gemeld dient te worden. Deze categorie staat in direct verband met de meldplicht van datalekken als genoemd in artikel 34a van de Wet Bescherming Persoonsgegevens. Deze categorie bestaat uit twee onderdelen. In het eerste onderdeel wordt geregeld op welke manier een datalek wordt gerapporteerd. Voor een dergelijke rapportage moet een procedure vastgesteld worden. Zwakke plekken in de beveiliging dienen door eenieder geregistreerd en gerapporteerd te worden. In het tweede onderdeel wordt beschreven hoe met een informatiebeveiligingsincident wordt omgegaan na de rapportage. Van informatiebeveiligingsincidenten dient geleerd te worden hoe met dergelijke incidenten in de toekomst omgegaan kan worden. Dit vereist een analyse van de situatie door middel van het verzamelen van bewijsmateriaal.

De negende categorie, Bedrijfscontinuïteitsbeheer, gaat over de manier waarop de bedrijfscontinuïteit gewaarborgd kan worden. Hierin staat vooral beschreven hoe data beveiligd kan worden tegen zaken die ervoor zouden zorgen dat de bedrijfsvoering niet door kan gaan, zoals storingen.

De tiende categorie, Naleving, gaat over het naleven van de wet- en regelgeving en huidig beleid. Deze categorie bestaat uit drie onderdelen. In het eerste onderdeel staat beschreven hoe voorkomen dient te worden dat er een schending van enige wet- of regelgeving plaatsvindt. Dit gebeurt vooral door gebruik te maken van een lijst van relevante wetgevingen. In het tweede onderdeel staat beschreven op welke manier de gemeente ervoor zorgt dat hun opgestelde beleid voldoende nageleefd wordt. Het derde onderdeel beschrijft hoe audits gebruikt kunnen worden om ervoor te zorgen dat alle informatiesystemen naar behoren werken en voldoen aan het bestaande beleid.

§3.2 Gemeente Schijndel

Binnen de gemeente Schijndel wordt databeveiliging in essentie geregeld op basis van twee documenten. Het eerste document is het Informatiebeveiligingsbeleid van de gemeente Schijndel voor de periode 2015 tot en met 2018. Dit informatiebeveiligingsbeleid is gebaseerd op de Strategische BIG van de IBD. Het tweede document is de Tactische Baseline gemeente Schijndel. Deze tactische baseline is grotendeels gebaseerd op de Tactische BIG van de IBD en voorziet in zekere zin als een uitbreiding op het informatiebeveiligingsbeleid.

§3.2.1 Informatiebeveiligingsbeleid

Het doel van dit beleidsplan is ‘het borgen van betrouwbare dienstverlening en het borgen van een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving[36]’.

De eerste relevante tekst in dit beleidsplan gaat over de ‘scope’, ofwel de reikwijdte van het beleid. Dit informatiebeveiligingsbeleid ziet toe op ‘alle bedrijfsvoeringsprocessen, onderliggende informatiesystemen en informatie van de gemeente’, ‘alle (fysieke) ruimten van een gemeentehuis en aanverwante gebouwen’, inclusief alle aanverwante apparatuur en de digitale omgeving van de gemeente[37].

In het beleidsplan is eveneens opgenomen wie welke verantwoordelijkheden heeft op het gebied van databeveiliging binnen de gemeente Schijndel. Primair is het ieders taak om te zorgen voor een goede informatiebeveiliging binnen de gemeente Schijndel. De medewerkers dienen zich integer te gedragen en geheimhouding in acht te nemen waar nodig[38]. Deze vereisten zijn eveneens opgenomen in de gedragscode integriteit van de gemeente Schijndel. Ook dienen de medewerkers te zijn opgeleid in het gebruik van informatiesystemen en andere informatiebronnen.

Naast deze verplichting die geldt voor alle medewerkers zijn er ook een aantal medewerkers die specifieke verantwoordelijkheden hebben op het gebied van databeveiliging. Allereerst draagt de algemeen directeur de eindverantwoordelijkheid voor de informatiebeveiliging. Ten tweede draagt de verantwoordelijke portefeuillehouder de bestuurlijke verantwoordelijkheid. Ten derde hebben alle informatiebronnen en –systemen een proceseigenaar die verantwoordelijk is voor de beveiliging van de informatie die hierin is opgeslagen. Ten slotte

[36] Informatiebeveiligingsbeleid 2015-2018 van de gemeente Schijndel, p. 4
[37] Informatiebeveiligingsbeleid 2015-2018 van de gemeente Schijndel, p. 4
[38] Informatiebeveiligingsbeleid 2015-2018 van de gemeente Schijndel, p. 5

is de Chief Information Security Officer (hierna: CISO) verantwoordelijk voor de uitvoering van het beleid. Ook geeft zij, gevraagd en ongevraagd, het management advies en feedback omtrent databeveiliging.

Indien gevoelige gegevens in de handen van derden komen valt dit ook onder de Wet Meldplicht Datalekken. Dit wordt dan ook onderzocht. Wanneer de oorzaak is gevonden, verholpen, en de omvang van het lek is gekwalificeerd en gekwantificeerd, wordt dit op een open manier gecommuniceerd met betrokken personen en instanties[39].

§3.2.2 Tactische Baseline informatiebeveiliging

De Tactische Baseline Informatiebeveiliging van de gemeente Schijndel is gebaseerd op de algemene tactische BIG van de IBD. De inhoud hiervan is reeds in paragraaf 3.1.1 besproken. Om die reden zal in deze paragraaf enkel besproken worden welke wijzigingen binnen de gemeente Schijndel hierin zijn aangebracht.

Het eerste, en grootste, verschil is dat in de Tactische Baseline Informatiebeveiliging van de gemeente Schijndel de hoofdstukken één tot en met vijf van de algemene Tactische BIG niet zijn opgenomen. Deze hoofdstukken gaan in op de implementatie en uitvoering van de Tactisch BIG en hoeven dus in een dergelijk document binnen een gemeente niet opgenomen te worden, zolang ze maar gebruikt worden. De hoofdstukken 6 tot en met 15 van de algemene Tactische BIG zijn in de gemeente Schijndel dan ook opnieuw genummerd als de hoofdstukken 1 tot en met 10.

Het tweede verschil staat in hoofdstuk 5, paragraaf 1 van de Tactische Baseline Databeveiliging Schijndel (hoofdstuk 10 van de algemene tactische BIG), onder het kopje ‘Scheiding van faciliteiten voor ontwikkeling, testen en productie’. Na de zin ‘Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test en/of Acceptatie en Productie (OTAP)’ in de algemene tactische BIG is in de Tactische Baseline Informatiebeveiliging Schijndel de tekst ‘voor kritieke informatiesystemen’ toegevoegd, waardoor andere vereisten worden gesteld.

Het derde verschil staat in hoofdstuk 7, paragraaf 1 van de Tactische Baseline Databeveiliging Schijndel (hoofdstuk 12 van de algemene tactische BIG), onder het kopje ‘Analyse en specificatie van beveiligingseisen’. In de algemene Tactische BIG staat dat voor elk project een beveiligingsrisicoanalyse en maatregelbepaling noodzakelijk is. Bij de gemeente Schijndel is dit alleen nodig bij ICT gerelateerde projecten.

§3.3 Gemeente Sint-Oedenrode

Binnen de gemeente Sint-Oedenrode wordt databeveiliging geregeld op basis van het Informatiebeveiligingsbeleid van de gemeente Sint-Oedenrode voor de periode 2014 tot en met 2017. Dit informatiebeveiligingsbeleid is gebaseerd op de, reeds hierboven beschreven, Strategische en Tactische BIG van het IBD. Bij de gemeente Sint-Oedenrode zijn deze twee documenten, in tegenstelling tot de gemeente Schijndel, samengevoegd in één beleid.

Allereerst zijn het doel en de ‘scope’ van dit informatiebeveiligingsbeleid belangrijk om te vermelden. Het doel van het beleid is grotendeels gelijk aan het doel als genoemd in het

[39] Informatiebeveiligingsbeleid 2015-2018 van de gemeente Schijndel, p. 5

informatiebeveiligingsbeleid van de gemeente Schijndel. De gemeente Sint-Oedenrode heeft het doel samengevat in vier kernpunten. Deze kernpunten zijn: het behoud van beschikbaarheid/continuïteit, het behoud van integriteit/betrouwbaarheid, het behoud van vertrouwelijkheid/exclusiviteit en het behoud van controleerbaarheid. De scope is in beide documenten identiek.

Het informatiebeveiligingsbeleid van de gemeente Sint-Oedenrode wordt gewaarborgd door middel van een Plan-Do-Check-Act cyclus. Hierbij worden drie uitgangspunten gehanteerd. Allereerst het informatiebeveiligingsbeleid, dat om de 4 jaar vernieuwd wordt. Ten tweede het informatiebeveiligingsplan en de risicoanalyse, waarmee het informatiebeveiligingsbeleid om de één à twee jaar getoetst wordt aan de praktijk. Ten derde het plan van aanpak, dat voortkomt uit het hiervoor genoemde informatiebeveiligingsplan en risicoanalyse. Deze wordt vier à zes keer per jaar bijgesteld.

In hoofdstuk 4 van het 'Informatiebeveiligingsbeleid 2014-2017 gemeente Sint-Oedenrode' wordt gesproken over de manier waarop risico's van dataverlies met betrekking tot menselijk handelen worden gemitigeerd. Hieronder vallen onder andere menselijke fouten, diefstal, fraude en misbruik van voorzieningen. Op het gebied van personeel is in het algemene gedeelte het volgende geregeld. Allereerst is de leidinggevende verantwoordelijk voor databeveiliging omtrent het aangaan, wijzigen of beëindigen van een dienstverband of een overeenkomst met externe partijen. P&O houdt hierop toezicht. Ten tweede bepaalt de leidinggevende welke rol(len) de medewerkers moeten vervullen en welke autorisaties hiervoor nodig zijn. Ten derde gelden, bij een inbreuk op de beveiliging, voor de medewerkers de gebruikelijke disciplinaire maatregelen. Deze maatregelen zijn onder meer genoemd in het Ambtenarenreglement en gemeentelijke regelingen. Enkele voorbeelden van mogelijke maatregelen zijn een schriftelijke berisping, inhouding van salaris en ontslag[40].

Op het gebied van tewerkstelling is het volgende geregeld: Ten eerste dienen alle medewerkers, waar mogelijk met terugwerkende kracht, de ambtseed of -belofte af te leggen. Ten tweede worden alle medewerkers geacht te handelen volgens het integriteitsprotocol, dat aangeeft dat ze integer moeten handelen, waaronder ook geheimhouding valt. Ten derde dienen medewerkers, eenmalig of periodiek, een Verklaring Omtrent Gedrag te overleggen. Ten vierde wijst de leidinggevende nieuwe werknemers op eventueel aanvullende, specifieke gedragsregels met betrekking tot bepaalde informatiesystemen of afdelingen. Ten slotte worden alle medewerkers op de hoogte gebracht van de aanwezigheid van een gedragsprotocol.

Met betrekking tot externe partijen die toegang hebben tot vertrouwelijke informatie is het volgende geregeld: Ten eerste dienen zij een geheimhoudingsverklaring te ondertekenen. Ten tweede worden zij, net als vaste medewerkers, geacht te handelen conform de voorschriften zoals genoemd in het integriteitsprotocol. Ten derde wijst de leidinggevende ook externe partijen op eventuele aanvullende, specifieke gedragsregels met betrekking tot bepaalde informatiesystemen of afdelingen. Ten vierde dienen externe partijen eveneens een Verklaring Omtrent Gedrag te overleggen. Ten slotte worden ook externe werknemers op de hoogte gebracht van de aanwezigheid van een gedragsprotocol.

[40] Art. 81 lid 1 van het Algemeen Rijksambtenarenreglement

Daarnaast zijn de volgende zaken geregeld in hoofdstuk 4. Ten eerste heeft de gemeente Sint-Oedenrode geen ‘kwetsbare’ posities, maar kiezen ze in plaats daarvan voor een zorgvuldig plaatsingsproces op alle functies. Ten tweede is er een procedure voor het toewijzen van toegang tot locaties en informatiesystemen per werknemer. Ten derde dient er voor de werknemers sprake te zijn van opleiding en bewustwording, om het risico op een datalek te minimaliseren. De teamleider is veelal verantwoordelijk hiervoor. Ten slotte staat in dit hoofdstuk een procedure omtrent verdenkingen van verduistering of ander gedrag dat in strijd is met de interne regels. Met toestemming van de algemeen directeur of gemeentesecretaris kan gebruik worden gemaakt van verscheidene opsporingsmogelijkheden zoals (verborgen) camera’s, microfoons en loggegevens.

In hoofdstuk 5 wordt gesproken over de fysieke beveiliging van het terrein, de gebouwen en de informatiesystemen. In dit hoofdstuk zijn de volgende zaken omtrent de fysieke beveiliging geregeld: Ten eerste dient de omgeving door middel van toegangsbeveiligingen in de vorm van fysieke barrières, zoals gesloten deuren, beveiligd te zijn. Ten tweede dient er beveiliging van kantoren ruimten en faciliteiten te zijn om ervoor te zorgen dat onbevoegden niet in deze ruimtes naar binnen kunnen. Ten derde dient er bescherming te zijn tegen bedreigingen van buitenaf, zoals brand, overstromingen, aardbevingen etc. Ten vierde behoren er richtlijnen en fysieke bescherming te zijn voor het werken in beveiligde ruimten. Ten slotte dient de toegang tot openbare gebieden voor laden en lossen te worden beheerst.

In hoofdstuk 6 worden procedures omschreven ter beveiliging van apparatuur en ter voorkoming van verlies, schade, diefstal en onderbreking van de bedrijfsactiviteiten. Hierin worden de volgende zaken geregeld. Allereerst dient apparatuur zo geplaatst te worden dat ze beschermd is tegen schade en storing door risico’s van buitenaf. Ten tweede behoort apparatuur beschermd te worden tegen stroomuitval en andere storingen. Ten derde horen kabels beschermd te worden tegen interceptie of beschadiging. Ten vierde dient apparatuur op correcte wijze onderhouden te worden. Ten vijfde dient apparatuur buiten het terrein beveiligd te worden, waarbij rekening wordt gehouden met de specifieke risico’s van die locatie. Ten zesde dienen opslagmedia te worden gecontroleerd voor verwijdering om te voorkomen dat bestanden verloren gaan. Ten slotte is het niet toegestaan dat apparatuur, informatie of programmatuur van de organisatie zonder toestemming van de locatie wordt meegenomen.

In hoofdstuk 7 wordt beschreven hoe communicatie- en bedieningsprocessen beheert worden. In de eerste paragraaf wordt staat geschreven dat bedieningsprocedure gedocumenteerd behoren te worden, dat wijzigingen in ICT-voorzieningen en informatiesystemen beheerst horen te worden, dat taken en verantwoordelijkheidsgebieden gescheiden horen te worden en dat faciliteiten voor ontwikkeling, testen en productie gescheiden horen te worden. In de tweede paragraaf wordt uitgelegd hoe informatiebeveiliging wordt geregeld indien er sprake is van dienstverlening door een derde partij. Dit houdt in dat er voor moet worden gezorgd dat de derde partij de niveaus van databeveiliging implementeert, uitvoert en bijhoudt. Tevens houdt dit in dat de derde partij gecontroleerd wordt door de gemeente om zeker te weten dat zij voldoen aan de beveiligingseisen van de gemeente en dat de gemeente wijzigingen in de dienstverlening door derden beheerd. In de derde paragraaf staat vermeld dat het risico van systeemstoringen tot een minimum wordt beperkt door middel van capaciteitsbeheer om de

vereiste systeemprestaties te bewerkstelligen en dat er aanvaardingscriteria behoren te worden vastgesteld voor nieuwe informatiesystemen en upgrades voorafgaand aan hun acceptatie. In de vierde paragraaf staat geschreven dat er maatregelen ter detectie, preventie en herstel getroffen dienen te worden tegen virussen, dat er maatregelen getroffen dienen te worden ingevoerd om het bewustzijn van de gebruikers te vergroten en dat de eventuele mobile code geconfigureerd behoort te zijn zodat deze functioneert volgens een duidelijk vastgesteld beveiligingsbeleid. De vijfde paragraaf geeft aan dat er back-ups gemaakt dienen te worden van informatie en programmatuur en dat dezen regelmatig worden getest.

In hoofdstuk 8 wordt beschreven hoe netwerkbeveiliging beheert wordt. De eerste paragraaf geeft aan dat er procedures vastgesteld behoren te zijn voor het beheer van verwijderbare media. Verwijderbare media dient overeenkomstig deze procedure verwijderd te worden, er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie en dat systeemdocumentatie dient beschermd te worden tegen onbevoegde toegang. In de tweede paragraaf wordt aangegeven dat er procedures en overeenkomsten vastgesteld behoren te worden voor de uitwisseling van informatie en dat deze uit te wisselen informatie beschermd dient te worden. De derde paragraaf gaat over e-commerce, en is vrijwel identiek aan de regeling hieromtrent in de algemene Tactische BIG, met uitzondering van het feit dat hier een kleine hoeveelheid details in is toegevoegd. Hetzelfde geldt voor paragraaf vier, de controle op informatieverwerkingsactiviteiten.

In hoofdstuk 9 wordt beschreven hoe toegangsbeveiliging tot informatie wordt geregeld. Dit volledige hoofdstuk is bijna gelijk aan hoofdstuk 11 van de algemene tactische BIG, met als enige verschil dat de gemeente Sint-Oedenrode minder specifieke maatregelen heeft opgenomen in hun beleid. Ditzelfde geldt voor hoofdstuk 10 van de gemeente Sint-Oedenrode, dat grotendeels gelijk is aan hoofdstuk 12 van de algemene tactische BIG.

Hoofdstuk 11 van het Informatiebeveiligingsbeleid 2014-2017 van de gemeente Sint-Oedenrode gaat over hoe omgegaan wordt met beveiligingsincidenten. In de eerste paragraaf wordt de gebruikte definitie van een beveiligingsincident gegeven. Een beveiligingsincident is voor de gemeente Sint-Oedenrode ‘een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie of informatiesystemen in gevaar is of kan komen’. De term ‘beschikbaarheid’ staat voor ‘de garanties over het afgesproken niveau van dienstverlening en over de toegankelijkheid en bruikbaarheid van informatie(systemen) op de afgesproken momenten’. Dit is uiteraard nauw verwant aan het beginsel van bedrijfscontinuïteit. De term ‘integriteit’ staat voor ‘de juistheid, volledigheid en tijdigheid van informatie(systemen). De term ‘vertrouwelijkheid’ staat voor ‘exclusiviteit van informatie en privacybescherming’.

In de tweede paragraaf wordt aangegeven dat er een procedure is voor het omgaan met beveiligingsincidenten. Deze procedure is opgenomen in bijlage 2 van het Informatiebeveiligingsbeleid 2014-2017 van de gemeente Sint-Oedenrode. Deze procedure bestaat uit 4 stappen. De eerste stap, identificatie en melding/registratie van incidenten, houdt in dat een medewerker een beveiligingsincident zo snel mogelijk moet melden aan de CISO, waarna deze het beveiligingsincident registreert. De tweede stap, afhandeling incidenten, houdt in dat de CISO, in samenwerking met het betrokken afdelingshoofd en eventueel een specialist, het incident analyseert en het risico inschat. Daarna worden er

maatregelen getroffen die bij een dergelijk risico passen ten behoeve van het verminderen van de impact van het incident en om ervoor te zorgen dat de situatie niet escaleert. Ten slotte worden bedrijfsprocessen die stopgezet zijn vanwege dit incident opnieuw opgestart. De derde stap, kennisgeving, houdt in dat betrokkenen in kennis worden gesteld van het incident. De betrokken afdeling wordt in ieder geval op de hoogte gesteld. Indien er sprake is van een ernstige inbreuk van vertrouwelijkheid van persoonsgegevens wordt melding gemaakt bij het CBP. Indien verdere ondersteuning of assistentie nodig is wordt het IBD eveneens ingelicht. De vierde stap, rapportage en evaluatie, houdt in dat informatie over beveiligingsrelevante handelingen minimaal 2 keer per jaar door de beveiligingsbeheerders doorgenomen wordt, waarna deze informatie met de CISO wordt gedeeld.

De hoofdstukken 14 en 15 van het Informatiebeveiligingsbeleid 2014-2017 van de gemeente Sint-Oedenrode zijn bijna gelijk aan respectievelijk hoofdstuk 9 en 10 van de algemene Tactische BIG. Het enige verschil is, wederom, dat in de algemene Tactische BIG meer specifieke maatregelen staan.

§3.4 Gemeente Veghel

Binnen de gemeente Veghel wordt, net als in de gemeente Schijndel, databeveiliging op basis van twee documenten geregeld, het Informatiebeveiligingsbeleid 2014-2017 en de Tactische Baseline Informatiebeveiliging van de gemeente Veghel.

§3.4.1 Informatiebeveiligingsbeleid

Wederom zal eerst gekeken worden naar het doel en de ‘scope’ van het Informatiebeveiligingsbeleid. Het doel, als opgenomen in het Informatiebeveiligingsbeleid 2014-2017 van de gemeente Veghel, is identiek aan het doel als opgenomen in het Informatiebeveiligingsbeleid 2014-2017 van de gemeente Schijndel (het borgen van betrouwbare dienstverlening en het borgen van een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving’). De ‘scope’ is eveneens identiek (alle bedrijfsvoeringsprocessen, onderliggende informatiesystemen en informatie van de gemeente, alle (fysieke) ruimten van een gemeentehuis en aanverwante gebouwen, inclusief alle aanverwante apparatuur en de digitale omgeving van de gemeente).

De verantwoordelijkheden binnen de gemeente Veghel zijn grotendeels gelijk aan die binnen de gemeente Schijndel. In het Informatiebeveiligingsbeleid van de gemeente Veghel staat echter één extra regel: ‘binnen elke afdeling is er één persoon aanwezig die tezamen met de informatiebeveiligingscoördinator het team informatiebeveiliging vormen. Dit team is verantwoordelijk voor uitdraging van het beleid, (mede) adviseren binnen de lijn en het afhandelen van beveiligingsincidenten’. Wanneer beveiligingsincidenten plaatsvinden worden deze verder gemeld bij de betrokken teamleider/manager en het team informatiebeveiliging die vervolgens actie ondernemen.

§3.4.2 Tactische Baseline Informatiebeveiliging

De Tactische Baseline Informatiebeveiliging van de gemeente Veghel is, net als die van de gemeente Schijndel, sterk gebaseerd op de Tactische BIG van het IBD. Om deze reden zijn deze documenten lijken deze documenten erg op elkaar. Hieronder zal aangegeven worden waar de belangrijkste verschillen zitten. Net als de binnen de gemeente Schijndel zijn in de Veghelse versie van de Tactische Baseline Informatiebeveiliging de hoofdstukken één tot en met vijf, zoals die in de algemene versie staan, niet opgenomen.

Het eerste verschil staat in hoofdstuk 1 paragraaf 1. Hoewel in de algemene versie van de Tactische BIG het college van B&W verantwoordelijk is voor het waarborgen van het vaststellen van de informatiedoelstellingen is dit in de gemeente Veghel de verantwoordelijk portefeuillehouder.

Het tweede verschil is dat de Tactische Baseline van de gemeente Veghel een vereiste heeft opgenomen in hoofdstuk 1 paragraaf 1 dat iedere ambtenaar een integriteitsverklaring dient te ondertekenen, in tegenstelling tot de geheimhoudingsverklaring die de algemene versie van de Tactische BIG vereist.

Het derde verschil is dat in hoofdstuk 3 paragraaf 1, naast de vereisten met betrekking tot Verklaringen Omtrent Gedrag, in de Tactische Baseline van de gemeente Veghel is opgenomen dat er maatregelen zijn vastgelegd wanneer een periodieke Verklaring Omtrent Gedrag of Verklaring van Geen Bezwaar niet kan worden afgelegd.

Het vierde verschil is dat in hoofdstuk 3 paragraaf 2, waarin regels zijn opgenomen omtrent bewustwording, binnen de gemeente Veghel is toegevoegd dat het onderwerp informatiebeveiliging als vastgesteld agendapunt tijdens een periodiek afdelings- en/of teamoverleg besproken dient te worden.

Het vijfde verschil is dat in hoofdstuk 4 paragraaf 1 van de Tactische BIG van de gemeente Veghel een andere verdeling van beveiligingszones wordt gemaakt dan de verdeling beschreven in de algemene versie van de Tactische BIG. De term ‘spreekkamers’, zoals gebruikt in de algemene versie van de Tactische BIG en welke vallen onder zone 1, is in de Tactische BIG van de gemeente Veghel opgedeeld in openbare en niet-openbare spreekkamers. Openbare spreekkamers vallen nog steeds onder zone 1, maar niet-openbare spreekkamers zijn in plaats daarvan opgeschaald naar zone 2.

Het zesde verschil staat eveneens in hoofdstuk 4 paragraaf 1. Met betrekking tot beveiligde ruimten staat in de algemene versie van de Tactische BIG dat beveiligde ruimten waarin zich geen personen bevinden zijn afgesloten en regelmatig worden gecontroleerd. In de Tactische BIG van de gemeente Veghel is de regelmatige controle echter niet opgenomen.

Het zevende verschil is dat in hoofdstuk 4 paragraaf 2, met betrekking tot plaatsing en bescherming van apparatuur, in de Tactische Baseline van de gemeente Veghel het verbod op eten en drinken is uitgebreid van ‘computerruimtes’ naar ‘zone 3’.

Het achtste verschil heeft betrekking tot opslagmedia zoals genoemd in hoofdstuk 4 paragraaf 2. Het gebruik van flash geheugen (e.g. SSD harddisks, geheugensticks) is, op grond van de Tactische BIG van de gemeente Veghel, verboden voor het opslaan van klasse II of III informatie, omdat deze geen veilige verwijder methoden ondersteunen.

Het negende verschil staat in hoofdstuk 5 paragraaf 1 en gaat over de functiescheiding. De Tactische BIG van de gemeente Veghel voegt op het gebied van functiescheiding enkele specifieke maatregelen toe. Deze maatregelen maken het onmogelijk om als beheerder gebruikerstaken uit te voeren, de eis dat wachtwoorden van gebruikersaccounts en

beheerdersaccounts niet hetzelfde zijn en dat wachtwoorden van beheerdersaccounts minimaal aan dezelfde vereisten moeten voldoen als wachtwoorden van gebruikersaccounts.

Het tiende verschil staat in hoofdstuk 5 paragraaf 4. Bij de tekst omtrent maatregelen tegen mobile code is in de Tactische Big van de gemeente Veghel toegevoegd dat de beperkingen centraal afgedwongen en beheerd dienen te worden, en dat deze onderhevig zijn een continue controle.

Het elfde verschil staat in hoofdstuk 5 paragraaf 7. Met betrekking tot systeemdocumentatie mag de eigenaar geen gerubriceerde systeemdocumentatie buiten de gemeente brengen zonder een risicoafweging. In de Tactische BIG van de gemeente Veghel is hier eveneens het vereiste aan toegevoegd dat de CISO geïnformeerd wordt.

Het twaalfde verschil staat in hoofdstuk 6 paragraaf 2. Met betrekking tot wachtwoorden is een wachtwoord in de gemeente Veghel 90 dagen geldig en mag deze niet binnen 10 keer herhaald worden. Bij de algemene versie van de Tactische BIG is dit 60 dagen en mag deze niet binnen 6 keer herhaald worden. Bovendien worden gebruikers en beheerders binnen de gemeente Veghel gefaciliteerd met een beveiligd wachtwoord management systeem.

Het dertiende verschil staat in hoofdstuk 7 paragraaf 3. Met betrekking tot sleutelbeheer dient er een procedure te bestaan omtrent gecompromitteerde sleutels. In de Tactische Baseline van de gemeente Veghel is hieraan toegevoegd dat in deze procedure in ieder geval de verplichting tot het bestaan van uitwijksleutels moet zijn vastgelegd.

Het veertiende verschil staat in hoofdstuk 7 paragraaf 4 onder het kopje ‘bescherming van testdata. Het gebruik van kopieën van operationele databases voor testgegevens dient vermeden te worden. In de Tactische Baseline van de gemeente Veghel is hieraan toegevoegd dat hier alleen vanaf geweken mag worden in overleg met de eigenaar van de informatie en dat hij of zij ermee akkoord moet gaan.

Het vijftiende verschil staat in hoofdstuk 8 paragraaf 1 onder het kopje ‘Rapportage van informatiebeveiligingsgebeurtenissen’. Hoewel een rapportage van een informatiebeveiligingsgebeurtenis ook volgens de algemene versie van de Tactische BIG noodzakelijk is voegt de gemeente Veghel hier nog een aantal vereisten aan toe. Allereerst staat in de Tactische BIG van de gemeente Veghel dat er per afdeling een contactpersoon moet zijn, terwijl er bij de gemeente Schijndel maar één contactpersoon in totaal is. Ten tweede wordt het systeem, waarin de beveiligingsincidenten worden vastgelegd, in Veghel niet doorgegeven aan de informatiebeveiligingsdienst maar aan de CISO, tenzij er sprake is van ‘ernstige gevallen waarbij netwerken, systemen of gegevens buiten de gemeente betrokken zijn’.

Het laatste verschil staat in hoofdstuk 10 paragraaf 1, onder het kopje; ‘Identificatie van toepasselijke wetgeving’. De gemeente Veghel voegt hieraan toe dat de vaststelling van relevante wetten minimaal één maal per jaar wordt gecontroleerd op actualiteit en bijgewerkt wordt waar dat nodig is.

Hoofdstuk 4: Beoordeling van het beleid

In dit hoofdstuk zal gekeken worden naar de vereisten waar het beleid van de gemeenten aan moet voldoen met betrekking tot databeveiliging en datalekken. Eerder is al gekeken naar het juridisch kader en naar het beleid van de drie te fuseren gemeenten. Nu is het van belang om dit beleid te toetsen aan het eerder opgestelde juridisch kader. Daarbij wordt er gekeken of het beleid van de drie te fuseren gemeenten wel doelmatig is en hoe dit gecontroleerd kan worden.

In dit hoofdstuk zal de volgende deelvraag worden beantwoord: *'In hoeverre zijn het huidige beleid, de processen en de protocollen met betrekking tot databeveiliging en datalekken van de drie te fuseren gemeenten rechtmatig en doelmatig en in hoeverre worden dezen nageleefd?'*

In dit hoofdstuk zal het hiervoor beschreven beleid van de drie te fuseren gemeenten nader onder de loep genomen worden. Hierbij zal gekeken worden naar drie deelonderwerpen. Allereerst zal gekeken worden of het opgestelde beleid ook daadwerkelijk uitgevoerd wordt zoals het beschreven staat. Immers, als het beleid niet wordt uitgevoerd heeft deze geen feitelijke waarde. Ten tweede zal gekeken worden of het opgestelde beleid van de drie te fuseren gemeenten voldoet aan de juridische eisen omtrent databeveiliging en datalekken. Ten derde zal gekeken worden of het opgestelde beleid van de drie te fuseren gemeenten doelmatig is. Indien het beleid juridisch correct is en goed wordt uitgevoerd dient immers gekeken te worden of het beleid wel doet wat het zou moeten doen en hoe dit gecontroleerd kan worden.

Aangezien deze deelvraag bestaat uit zowel juridische als praktijkgerichte onderdelen dient gebruik gemaakt te worden van de onderzoeksmethoden 'rechtsbronnen- en literatuuronderzoek' en een 'kwalitatief praktijkonderzoek'. Ten eerste dient, door middel van een kwalitatief praktijkonderzoek, gekeken te worden of het beleid goed wordt uitgevoerd. Dit kan enkel in de praktijk onderzocht worden en daarom is voor dit onderdeel een 'kwalitatief praktijkonderzoek' dan ook de enige logische keuze. Ten tweede dienen rechtsbronnen en literatuur gebruikt te worden om de vraag te beantwoorden of het beleid van de drie te fuseren gemeenten voldoen aan de wettelijke vereisten. Voor dit onderdeel is een 'rechtsbronnen- en literatuuronderzoek' dan ook de enige logische keuze. Ten derde dient gebruik gemaakt te worden van zowel praktijkonderzoek als literatuuronderzoek om te controleren of het bestaande beleid voldoende doelmatig is. Aan de ene kant dient immers gekeken te worden naar de praktijksituatie, maar aan de andere kant moet literatuur bestudeerd worden met betrekking tot het opzetten van een kwaliteitskader. Op de rechtsbronnen en literatuur die voor het beantwoorden van deze deelvraag gebruikt zal worden zal de inhoudsanalyse worden toegepast. Dit is immers de enige logische keuze voor een dergelijke onderzoeksmethode. Op de onderdelen waarbij een kwalitatief praktijkonderzoek wordt toegepast zal gebruik gemaakt worden van enerzijds de casestudy, die belangrijk is voor de onderdelen die ingaan op de beoordeling van het beleid en anderzijds van een kwalitatieve survey, waarmee gekeken zal worden hoe het beleid ten uitvoer wordt gebracht.

De belangrijkste bronnen voor het beantwoorden van deze deelvraag zijn als volgt. Op het gebied van rechtsbronnen-onderzoek is de Wet Bescherming Persoonsgegevens, waarvan

specifiek de artikelen 13, die ingaat op databeveiliging, en 34a, die ingaat op het melden van datalekken, vooral relevant. Op het gebied van kwalitatief praktijkonderzoek zal hoofdzakelijk gebruik gemaakt worden van het beleid van de drie te fuseren gemeenten, de CISO's van de drie te fuseren gemeenten en medewerkers van die gemeenten.

De antwoorden die voortkomen uit dit hoofdstuk zullen, in combinatie met eerdere hoofdstukken, de basis vormen voor het beantwoorden van de centrale vraag van dit onderzoek.

§4.1 Uitvoering van het beleid

Allereerst zal gekeken worden naar hoe het beleid van de drie te fuseren gemeenten in de praktijk ten uitvoer wordt gebracht. Hier zal per gemeente naar worden gekeken op basis van twee vragenlijsten (zie bijlagen 1 en 2). De eerste vragenlijst, die bestemd is voor de CISO's van de drie te fuseren gemeenten, is afgenomen in de vorm van een open interview. De tweede vragenlijst, die bestemd is voor andere werknemers van de gemeenten, is afgenomen in de vorm van een enquête.

§4.1.1 Gemeente Schijndel

Binnen de gemeente Schijndel is Anouk Vlemmix geïnterviewd. Op de eerste vraag, waarom is gekozen voor de BIG van de IBD, gaf zij het volgende antwoord:

"Omdat er destijds een verdrag is ondertekend waarin de burgemeesters van de Nederlandse gemeenten hebben aangegeven dat ze die baseline gaan volgen. Het beleid van de gemeente Schijndel is daar ook op afgestemd. Zij hebben hiervoor gekozen om het informatiebeveiliging binnen de organisaties goed te gaan regelen en waarborgen."

Op de tweede vraag: zijn de zaken die geregeld 'behoren' te worden ook daadwerkelijk geregeld en is over de zaken waarover geïnformeerd 'dient' te worden ook daadwerkelijk geïnformeerd, antwoordde zij als volgt:

"Sommige dingen doen we als gemeente al wel, andere dingen moeten nog gedaan worden. Voor 2016 is een informatiebeveiligingsplan opgesteld, waarin staat welke punten we dit jaar gaan uitvoeren en welke maatregelen van de BIG hieraan verbonden zijn. Nog niet alles is dus geregeld maar we zijn er wel mee bezig. Dat wil zeggen, we zullen er tot de fusie mee bezig blijven."

Op de derde vraag of het beleid sinds zijn invoering al is aangepast, gaf zij het volgende antwoord:

"Nee, het beleid is pas eind vorig jaar vastgesteld en is dus nog niet aangepast."

Uit de enquête die afgenomen is bij de medewerkers van de gemeente Schijndel is het volgende gebleken:

Binnen de gemeente Schijndel is ongeveer 79 procent van de respondenten zich bewust van het bestaan van een databeveiligingsbeleid. Hiervan zegt 50 procent de inhoud van dit beleid niet te kennen, 38 procent zegt de inhoud redelijk te kennen en slechts 12 procent geeft aan dat hij volledig bekend is met de inhoud.

Van de 79 procent van de werknemers die zegt zich bewust te zijn van het informatiebeveiligingsbeleid zegt 60 procent dat zij er niet actief voor zorgen dat zij aan dit beleid voldoen, tegenover 40 procent die zegt dat wel te doen.

Van alle werknemers binnen de gemeente Schijndel geeft 58 procent dat zij actief bezig zijn met de beveiliging van informatie. De overige 42 procent is hier niet actief mee bezig.

Met betrekking tot communicatie vindt slechts 21 procent van de ondervraagden dat er goed gecommuniceerd wordt wat van hen wordt verwacht met betrekking tot databeveiliging. De overige 79 procent vindt dat de communicatie hieromtrent niet voldoende (27 procent), of zelfs ronduit slecht is (52 procent).

Wanneer gevraagd wordt hoe de communicatie omtrent databeveiliging mogelijk beter kan worden verschillende antwoorden gegeven. De meest terugkerende punten in deze antwoorden zijn dat er meer op gecontroleerd zou moeten worden, dat de medewerkers een persoonlijke aanpak zouden prefereren en dat in ieder geval duidelijk gecommuniceerd moet worden wat van hen specifiek wordt verwacht, in ieder geval met betrekking tot de belangrijkste punten. Met betrekking tot de vraag of dit fysiek of digitaal moet gebeuren zijn de meningen verdeeld.

§4.1.2 Gemeente Sint-Oedenrode

Binnen de gemeente Sint-Oedenrode is Anke Hobbelen geïnterviewd. Op de eerste vraag: waarom is gekozen voor de BIG van de IBD, gaf zij het volgende antwoord:

“Wij hebben daarvoor gekozen omdat dat beleid eigenlijk al vrij goed uitgewerkt was. Bovendien is het op die manier makkelijker. Je kunt beter iets gebruiken dat al bestaat en waarover nagedacht is dan dat je zelf iets moet verzinnen. Het is aanvankelijk ontstaan vanuit een noodzaak; Een audit die we kregen toen we nog geen beleid hadden. Qua tijd was het dus noodzakelijk om snel iets te regelen. Het is uiteraard wel belangrijk, maar we hebben nog te weinig tijd gehad om het goed uit te voeren.”

Op de tweede vraag: zijn de zaken die geregeld ‘behoren’ te worden ook daadwerkelijk geregeld en is over de zaken waarover geïnformeerd ‘dient’ te worden ook daadwerkelijk geïnformeerd, antwoordde zij als volgt:

“Sommige gedeelten al wel, anderen nog niet. Het is op dit moment nog zo dat het vaker niet geregeld is dan dat het wel geregeld is. Dit is omdat er gewoon nog te weinig op gecontroleerd wordt, waardoor niet aangegeven wordt waar het gecorrigeerd moet worden. Het schort nog in de uitvoering en de controle. Dat heeft ook vooral te maken met de tijd en de aanstaande fusie.”

Op de derde vraag: of het beleid sinds zijn invoering al is aangepast, gaf zij het volgende antwoord:

“Nee, omdat we wisten dat Meierijstad eraan kwam en het dan uitgebreid onder de loep wordt genomen. We hebben ervoor gekozen om het tot die tijd slechts minimaal uit te voeren. We hebben wel veel gefocust op awareness.”

Uit de enquête die is afgenomen bij de medewerkers van de gemeente Sint-Oedenrode is het volgende gebleken:

Meer dan 93 procent van de werknemers van de gemeente Sint-Oedenrode is zich ervan bewust dat er een informatiebeveiligingsbeleid is. Hiervan geeft slechts 7 procent aan dat zij de inhoud van het beleid goed kennen, 43 procent geeft aan dat zij de inhoud van het informatiebeveiligingsbeleid in zijn geheel niet kennen en 50 procent geeft aan de inhoud van het beleid gedeeltelijk te kennen.

Van de werknemers die zeggen zich bewust te zijn van het informatiebeveiligingsbeleid zegt iets meer dan 57 procent dat zij er actief voor zorgen dat zij, en mogelijk hun afdeling, voldoen aan de hierin gestelde eisen. Ruim 73 procent van alle werknemers binnen de gemeente Sint-Oedenrode geeft aan dat zij actief bezig zijn met de beveiliging van informatie.

Met betrekking tot communicatie vindt slechts 20 procent van de ondervraagden dat er goed gecommuniceerd wordt over wat er van hen wordt verwacht wordt met betrekking tot databeveiliging. De overige 80 procent vindt dat de communicatie hieromtrent niet voldoende (37 procent), of zelfs ronduit slecht is (43 procent).

Wanneer gevraagd wordt hoe de communicatie omtrent databeveiliging mogelijk beter kan worden hoofdzakelijk twee soorten antwoorden gegeven. Veel medewerkers geven aan dat de communicatie duidelijk op één plek beschikbaar moet zijn. Ook geven veel medewerkers aan dat hier periodiek aandacht aan moet worden besteedt, omdat de kennis wegzakt.

§4.1.3 Gemeente Veghel

Binnen de gemeente Veghel is Ruud van Oorschot geïnterviewd. Op de eerste vraag: waarom is gekozen voor de BIG van de IBD, gaf hij het volgende antwoord:

“De BIG is in principe een aanpassing van een oudere ISO-norm om beter van toepassing te zijn op gemeentelijke problematiek. Wij verwachtten dat deze BIG over enkele jaren de norm wordt voor databeveiliging binnen gemeenten. Er is dus hiervoor gekozen omdat de gemeente dan is voorbereid wanneer dit wordt ingevoerd. Verder schat ik in dat, op termijn, binnen gemeenten het ‘single-audit’ principe wordt ingevoerd. In dat geval is het goed om een tactische baseline te hebben die overal voor geldt. Verder is de ISO-norm een goede internationale standaard voor databeveiliging.”

Op de tweede vraag: zijn de zaken die geregeld ‘behoren’ te worden ook daadwerkelijk geregeld en is over de zaken waarover geïnformeerd ‘dient’ te worden ook daadwerkelijk geïnformeerd, antwoordde zij als volgt:

“Hetgeen in de BIG is opgenomen is ‘best practice’. Dit wil je uiteindelijk bereiken. Tot die tijd wil je jezelf niet beperken in wat je hiermee kunt. Een dergelijk beleidsstuk wordt vastgesteld door het college van B&W. De raad heeft hier soms ook nog iets over te zeggen. Het is niet praktisch om alles direct te proberen te regelen. Die terminologie in de BIG wordt gebruikt om speelruimte te creëren. Binnen die tijd heb je vervolgens de tijd om er iets aan te doen. Niet alles wat in de baseline is opgenomen is al geïmplementeerd, wat onder andere door de

fusie komt. Met betrekking tot de genoemde kwalificatie van informatie zijn er al wel richtlijnen."

Op de derde vraag: of het beleid sinds zijn invoering al is aangepast, gaf hij het volgende antwoord:

"Nee, het beleid op zichzelf is nog niet aangepast. Er zijn wel procedures en dergelijke bijgekomen en gewijzigd, waarvan sommige jaarlijks tegen het licht worden gehouden. Het beleid zelf is dus niet gewijzigd, maar de uitwerking ervan wel".

Uit de enquête die is afgenomen bij de medewerkers van de gemeente Veghel is het volgende gebleken:

Ruim 93 procent van de werknemers van de gemeente Veghel is zich ervan bewust dat er een informatiebeveiligingsbeleid is. Hiervan kent ongeveer 15 procent de inhoud goed, ongeveer 62 procent zegt de inhoud redelijk te kennen en 23 procent geeft aan dat hij volledig onbekend is met de inhoud.

Van de 90 procent van de werknemers die zegt zich bewust te zijn van het informatiebeveiligingsbeleid zegt iets meer dan de helft dat zij er actief voor zorgen dat zij, en mogelijk hun afdeling, voldoen aan de hierin gestelde eisen.

Van alle werknemers binnen de gemeente Veghel zegt ruim 80 procent dat zij actief bezig zijn met de beveiliging van informatie.

Met betrekking tot communicatie vindt slechts 33 procent van de ondervraagden dat er goed gecommuniceerd wordt over wat er van hen verwacht wordt met betrekking tot databeveiliging. De overige 67 procent vindt dat de communicatie niet voldoende (54 procent), of zelfs ronduit slecht is (13 procent). Opvallend is dat de gemeente Veghel de enige van de drie gemeenten is waarbij de groep die de communicatie onvoldoende vindt voor het grootste deel bestaat uit medewerkers die van mening zijn dat de communicatie redelijk is i.p.v. slecht.

Wanneer gevraagd wordt hoe de communicatie omtrent databeveiliging mogelijk beter kan worden de meest uiteenlopende antwoorden gegeven. Over het algemeen gaan de antwoorden in op drie kernpunten. Het eerste punt dat vaak wordt genoemd is dat dergelijke communicatie structureel moet gebeuren. Het tweede punt dat vaak wordt genoemd is dat de communicatie zodanig moet zijn dat je er niet omheen kunt. De suggesties hieromtrent variëren van post-its op de computerschermen tot posters in de gangen. Het derde punt dat vaak wordt genoemd is dat bij de communicatie ook aandacht moet worden besteed aan praktische toepasbaarheid. Dit houdt in dat werknemers graag willen weten hoe de regels op hun werk van toepassing zijn en hoe zij hieraan kunnen voldoen.

§4.2 Rechtmatigheid van het beleid

Voordat de rechtmatigheid van het beleid van de drie gemeenten op het gebied van databeveiliging en het melden van datalekken beoordeeld zal worden zal eerst kort uiteengezet worden waar het beleid aan moet voldoen. In essentie moet het beleid op grond van de Wet Meldplicht Datalekken twee zaken bevatten. Ten eerste moeten, op grond van

artikel 13 van de Wet Bescherming Persoonsgegevens, passende technische en organisatorische maatregelen genomen worden om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Ten tweede moet, op grond van artikel 34a, een datalek in de meeste gevallen gemeld worden aan de Autoriteit Persoonsgegevens en in sommige gevallen ook aan de betrokkene. Voor een dergelijke melding zijn een aantal vereisten, die in hoofdstuk 2 reeds zijn besproken.

Met betrekking tot de beveiliging van data zal enkel gesproken worden over de organisatorische maatregelen. De reden hiervoor is dat de technische maatregelen moeilijker te achterhalen zijn en deze, vanwege hun complexiteit, vrijwel onmogelijk te beoordelen zijn.

Het is erg gecompliceerd om de rechtmatigheid van de organisatorische databeveiligingsmaatregelen te beoordelen. In de wet en de memorie van toelichting wordt namelijk enkel aangegeven dat de maatregelen een passend beveiligingsniveau moeten garanderen, gelet op de risico's van de verwerking en de aard van de te beschermen gegevens. Binnen gemeenten worden veel persoonsgegevens verwerkt met betrekking tot haar burgers, waaronder NAW-gegevens en burgerservicenummers. De aard van de te beschermen gegevens vereist dus dat het beveiligingsniveau hoog moet zijn. De eventuele gevolgen bij een datalek zijn immers ook extreem groot. Het is relevant om op te merken dat de KING, die de basis voor het databeveiligingsbeleid van de drie te fuseren gemeenten heeft opgesteld, een samenwerkingsverband is tussen verschillende partijen, waaronder de VNG. Dit, in combinatie met het feit dat alle gemeenten in Nederland deze baseline gebruiken[41], geeft vertrouwen dat deze baseline, mits goed uitgevoerd, voldoende rechtmatig is. Bovendien heeft minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties het volgende gezegd met betrekking tot dit onderwerp: 'Mij zijn dus geen gemeenten bekend die informatiebeveiliging in het algemeen of de beveiliging van persoonsgegevens in het bijzonder niet op orde zouden hebben[42]'.

§4.2.1 Gemeente Schijndel

Zoals in hoofdstuk 3 reeds uiteengezet is zijn de databeveiligingsmaatregelen in de gemeente Schijndel grotendeels gebaseerd op de BIG van KING. Deze maatregelen zien toe op de bescherming van persoonsgegevens door middel van het screenen, informeren en trainen van personeel, het beschermen van bepaalde beveiligde locaties tegen onrechtmatige betreding en het beveiligen van systemen tegen ongeoorloofde dataverwerking of dataverlies.

De aanpassingen van de gemeente Schijndel op deze baseline zijn beschreven in hoofdstuk drie. De eerste aanpassing limiteert het aantal logisch gescheiden systemen voor ontwikkeling, test en/of acceptatie en productie. Hierdoor is de beveiliging logischerwijs minder effectief, omdat deze zin als doel heeft om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen[43]'.

[41] Kamerstukken II 2015/16, 2 076, p. 2
[42] Kamerstukken II 2015/16, 2 076, p. 2
[43] Tactische Baseline Informatiebeveiliging Gemeenten, p. 52

De tweede aanpassing geeft de risicoanalyse bij bepaalde projecten op in ruil voor gebruiksvriendelijkheid. Dit kan eventueel een risico vormen voor de databeveiliging, omdat beveiligingsrisico's van dergelijke projecten niet worden gedocumenteerd.

Samengevat leveren deze twee aanpassingen door de gemeente Schijndel dus potentiële beveiligingsrisico's op.

Over de meldplicht datalekken op grond van artikel 34a van de Wet Bescherming Persoonsgegevens hoeft weinig gezegd te worden. Er is binnen de gemeente Schijndel geen procedure voor het melden van datalekken aan de Autoriteit Persoonsgegevens of aan de betrokkene(n). De mogelijkheid om deze op te stellen is echter wel opgenomen in de tactische baseline databeveiliging van de gemeente Schijndel in paragraaf 5.8 onder het kopje 'uitwisselingsovereenkomsten'. Er is een interne meldplicht voor datalekken die als doel heeft om zwakke punten in de beveiliging tijdig op te sporen en op te lossen. Deze procedure is opgenomen in paragraaf 8.1 van de Tactische Baseline Informatiebeveiliging Schijndel.

§4.2.2 Gemeente Sint-Oedenrode

Zoals in hoofdstuk 3 reeds uiteengezet is zijn de databeveiligingsmaatregelen in de gemeente Sint-Oedenrode grotendeels gebaseerd op de BIG van KING. Deze maatregelen zien toe op de bescherming van persoonsgegevens door middel van het screenen, informeren en trainen van personeel, het beschermen van bepaalde beveiligde locaties tegen onrechtmatige betreding en het beveiligen van systemen tegen ongeoorloofde dataverwerking of dataverlies.

Bij de gemeente Sint-Oedenrode is het kenmerkend dat het informatiebeveiligingsbeleid in vergelijking met de BIG van de IBD ingekort is. Zo zijn veel specificaties uit het origineel verwijderd uit de versie van Sint-Oedenrode. De reden hiervoor is dat de gemeente Sint-Oedenrode deze informatie heeft opgenomen in losse protocollen met betrekking tot databeveiliging. Dit is mogelijk een databeveiligingsrisico, aangezien nog niet alle processen en protocollen zijn opgesteld en er dus niets geregeld is tot die processen en protocollen worden opgesteld.

Eveneens opvallend is dat de versie van de Tactische Baseline Informatiebeveiliging van de gemeente Sint-Oedenrode meer toegespitst lijkt op de gemeente, waardoor bepaalde problemen die specifiek voor deze gemeente gelden beter behandeld kunnen worden.

De gemeente Sint-Oedenrode heeft slechts een minimale procedure voor het melden van datalekken aan de Autoriteit Persoonsgegevens. In hun interne procedure voor het melden van datelekken staat enkel dat bij een datalek waarbij 'sprake is van ernstige inbreuk van vertrouwelijkheid van persoonsgegevens' melding wordt gemaakt bij het College Bescherming Persoonsgegevens door de privacy beheerder[44]. Dit is echter onvoldoende, aangezien nergens wordt aangegeven wanneer er sprake is van een 'ernstige inbreuk van vertrouwelijkheid' en wat een dergelijke melding precies moet inhouden. Wel hebben zij, net als de gemeente Schijndel een interne procedure voor het melden van datalekken. Deze

[44] Informatiebeveiligingsbeleid 2014-2017 gemeente Sint-Oedenrode, p. 40

procedure is afgeleid van de procedure Incident management en Respons van de IBD uit 2013.

§4.2.3 Gemeente Veghel

Zoals in hoofdstuk 3 reeds uiteengezet is zijn de databeveiligingsmaatregelen in de gemeente Veghel grotendeels gebaseerd op de BIG van KING. Deze maatregelen zien toe op de bescherming van persoonsgegevens door middel van het screenen, informeren en trainen van personeel, het beschermen van bepaalde beveiligde locaties tegen onrechtmatige betreding en het beveiligen van systemen tegen ongeoorloofde dataverwerking of dataverlies.

De gemeente Veghel heeft een vrij groot aantal aanpassingen op de standaard BIG, die zijn beschreven in hoofdstuk 3. Het grootste deel van deze veranderingen is erop gericht om de maatregelen met betrekking tot databeveiliging verder te verscherpen. Zo zijn onder andere de zonebeveiligingsvereisten aangescherpt met betrekking tot fysieke toegang en wordt de relevante wet- en regelgeving vaker gecontroleerd dan in andere gemeenten.

Op bepaalde gebieden is het beleid van de gemeente Veghel ook iets versoepeld. Een voorbeeld hiervan is dat een wachtwoord in de gemeente Veghel 90 dagen geldig is, terwijl deze in de gemeente Schijndel maar 60 dagen geldig is. De reden hiervoor is dat een dergelijke regeling een grotere gebruiksvriendelijkheid met zich meebrengt. De eventuele beveiligingsrisico's die hieruit voortkomen worden gecompenseerd door het feit dat een wachtwoord pas na een langere periode herhaald mag worden (900 dagen in de gemeente Veghel tegenover 360 dagen in de gemeente Schijndel).

De gemeente Veghel heeft, net als de gemeente Schijndel geen enkele procedure voor het melden van datalekken aan de Autoriteit Persoonsgegevens of aan betrokkenen.

Hoofdstuk 5: Conclusies en aanbevelingen

In de vorige hoofdstukken is gesproken over de in de wet gestelde eisen met betrekking tot databeveiliging en datalekken, evenals het huidige beleid van de drie te fuseren gemeenten, en de praktische uitvoering, rechtmatigheid en doelmatigheid van dit beleid. Uit de informatie die hieruit is voortgekomen worden in dit hoofdstuk conclusies getrokken. Met behulp van deze conclusies kan de centrale vraag beantwoord worden.

In hoeverre zijn het beleid, de processen en de protocollen met betrekking tot databeveiliging en datalekken van de gemeenten Schijndel, Sint-Oedenrode en Veghel juridisch correct en voldoende doelmatig om opgenomen te worden in het toekomstige beleid, de processen en de protocollen van de fusiegemeente Meierijstad, gelet op de geldende wet- en regelgeving omtrent privacy?"

De antwoorden op deze vragen zullen leiden tot aanbevelingen die de gemeente Meijerijstad kan gebruiken om een beleid op te stellen over databeveiliging en het melden van datalekken welke voldoet aan de hieraan gestelde eisen in de Wet Bescherming Persoonsgegevens en welke in de praktijk adequaat uitgevoerd kan worden.

Dit hoofdstuk zal op de volgende manier opgebouwd worden. Allereerst zullen conclusies getrokken worden met behulp van de informatie die in eerdere hoofdstukken zijn verzameld. Er zal geconcludeerd worden of de drie te fuseren gemeenten voldoen aan de in de wet gestelde vereisten met betrekking tot databeveiliging en het melden van eventuele datalekken. Daarnaast zal gekeken worden of de werknemers zich bewust zijn van databeveiliging en hun taak daarin. Hierna zal antwoord worden gegeven op de hierboven genoemde centrale vraag. Ten slotte zullen aanbevelingen worden gedaan over hoe de drie gemeenten deze conclusies kunnen gebruiken in de overgang naar Meierijstad en waar ze vooral op moeten letten.

§5.1 Conclusies

§5.1.1 Voldoen de gemeenten aan de wettelijke vereisten omtrent databeveiliging?

Zoals in hoofdstuk 2 en in hoofdstuk 4 is aangegeven zijn de wettelijke vereisten met betrekking tot databeveiliging met opzet vaag gehouden om instanties die data verwerken meer beleidsvrijheid te geven en omdat de wetgeving anders sterk tijdgebonden zou zijn. Redelijkerwijs mag volgens minister Plasterk aangenomen worden dat een gemeente voldoet aan de eisen die gesteld worden met betrekking tot databeveiliging wanneer een gemeente de Baseline Informatiebeveiliging Gemeenten (BIG) van de Informatiebeveiligingsdienst (IBD) gebruikt, goed integreert en uitvoert. Gemeenten kunnen hun eigen versie van deze baseline maken om beter aan te sluiten bij hun belangen.

De gemeente Schijndel heeft de BIG van de IBD binnen de gemeente ingevoerd en deze wordt ook in de praktijk geïntegreerd en uitgevoerd. De gemeente Schijndel heeft twee aanpassingen gedaan in de Baseline. Deze aanpassingen hebben tot gevolg dat informatie minder goed beveiligd wordt dan wanneer de BIG van de IBD aangehouden werd. De met opzet vage formulering met betrekking tot databeveiliging in de Wet Bescherming Persoonsgegevens zorgt ervoor dat de gemeente Schijndel, ondanks deze aanpassingen, wel voldoet aan de hiervoor in de wet gestelde vereisten omtrent databeveiliging.

De gemeente Sint-Oedenrode heeft eveneens de BIG van de IBD binnen de gemeente ingevoerd en deze wordt ook in de praktijk geïntegreerd en uitgevoerd. Door de aanpassingen van de gemeente Sint-Oedenrode wordt het beleid ingekort en toegespitst op de gemeente. De aanpassingen omtrent het inkorten van de tactische baseline zorgen er mogelijk voor dat de persoonsgegevens minder goed beveiligd worden, hoewel dit vooral samenhangt met de uitvoering van het beleid. Ook de gemeente Sint-Oedenrode voldoet aan de in de Wet Bescherming Persoonsgegevens gestelde eisen omtrent databeveiliging omdat deze eisen opzettelijk vaag zijn gehouden.

De gemeente Veghel heeft, net als de gemeenten Schijndel en Sint-Oedenrode de BIG van de IBD binnen de gemeente ingevoerd. Ook in Veghel wordt deze in de praktijk geïntegreerd en uitgevoerd. De aanpassingen die de gemeente Veghel heeft gemaakt op de BIG van de IBD zijn in de meeste gevallen een kleine verbetering op het gebied van databeveiliging en in de overige gevallen neutraal of slechts lichtelijk negatief. Wanneer je deze veranderingen tegen elkaar wegstreept is het resultaat van de aanpassingen overwegend positief. De gemeente Veghel voldoet dus ruim aan de eisen omtrent databeveiliging zoals die genoemd zijn in de Wet Meldplicht Datalekken.

§5.1.2 Voldoen de gemeenten aan de wettelijke vereisten omtrent de meldplicht datalekken?

Zoals in hoofdstuk 2 reeds uiteen is gezet dienen dataverwerkers, waaronder gemeenten, een beleid te hebben voor het melden van datalekken aan de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen. Indien een dergelijk datalek niet wordt gemeld kan een gemeente een boete opgelegd krijgen van maximaal 820.000 euro.

De gemeenten Schijndel en Veghel voldoen niet aan de meldplicht datalekken. Deze gemeenten hebben namelijk geen beleid voor het melden van datalekken aan de Autoriteit Persoonsgegevens. Het beleid omtrent het melden van datalekken dat deze gemeenten wel hebben is grotendeels een interne meldplicht. Hoewel hierin is opgenomen dat het datalek onder bepaalde omstandigheden gecommuniceerd zal worden aan de betrokkene(n), zijn hier geen criteria voor opgenomen. Dit beleid voldoet dan ook niet aan de vereisten als genoemd in artikel 34a van de Wet Bescherming Persoonsgegevens.

Bij de gemeente Sint-Oedenrode is eveneens sprake van een vooral interne meldplicht. Binnen deze procedure is echter wel een beperkte externe meldplicht aan het College Bescherming Persoonsgegevens opgenomen. Dit is echter slechts één zin en hierin staan geen vereisten opgenomen. Ook deze meldplicht voldoet dus niet aan de vereisten zoals genoemd in artikel 34a van de Wet Bescherming Persoonsgegevens.

Geen van de drie te fuseren gemeenten voldoet dus aan de meldplicht datalekken zoals genoemd in artikel 34a van de Wet Bescherming Persoonsgegevens.

§5.1.3 Is het beleid van de drie gemeenten omtrent databeveiliging voldoende doelmatig?

Aangezien het databeveiligingsbeleid van de drie te fuseren gemeenten gebaseerd is op de BIG van de IBD zal bij de beoordeling van de doelmatigheid van het beleid vooral gelet worden op de aanpassingen die de gemeenten hierin zelf hebben aangebracht en het gebruiksgemak van het beleid.

De wijzigingen die de gemeente Schijndel heeft aangebracht in haar versie van de Tactische BIG zijn er specifiek op gericht om het uitvoeren van bepaalde onderdelen van deze tactische baseline makkelijker te maken en om, naar de mening van de gemeente Schijndel, onnodige processen uit te sluiten. De doelmatigheid van de Tactische baseline van de gemeente Schijndel is dan ook hoger dan die van de standaard versie.

De wijzigingen die de gemeente Sint-Oedenrode heeft aangebracht in haar versie van de Tactische baseline zijn grotendeels gericht op het inkorten van de Tactische baseline door het verwijderen van verklarende teksten. Op het gebied van doelmatigheid is het document makkelijker te lezen. Het is echter voor werknemers moeilijker om duidelijk te krijgen wat er specifiek van hen verwacht wordt. Hierdoor lijkt de versie van de gemeente Sint-Oedenrode iets minder doelmatig dan de standaardversie van de BIG.

De wijzigingen die de gemeente Veghel heeft aangebracht in haar versie van de Tactische BIG zorgen ervoor dat haar versie van de tactische BIG beter is ingericht om te voldoen aan de specifieke vereisten binnen de gemeente Veghel. Eveneens zorgen deze aanpassingen ervoor dat de Tactische BIG van de gemeente Veghel op bepaalde punten voor de werknemers is gewijzigd, zodat deze makkelijker uitvoerbaar is. De Tactische BIG van de gemeente Veghel is, van de drie te fuseren gemeenten, veruit het beste op het gebied van doelmatigheid.

§5.1.4 Wordt het beleid goed uitgevoerd?

In dit hoofdstuk is tot nu toe enkel gesproken over de inhoud van het beleid van de drie te fuseren gemeenten. Als het beleid binnen een gemeente echter niet of onvoldoende wordt uitgevoerd is het irrelevant of het beleid op zichzelf goed is of niet. Door middel van het interviewen van de CISO's van de te fuseren gemeenten en het afnemen van een enquête bij de medewerkers is meer informatie verzameld over hoe het beleid wordt uitgevoerd. Wat in deze interviews aan het licht is gekomen is reeds in hoofdstuk 4 besproken.

Binnen de gemeente Schijndel blijkt dat nog niet alles wat in de Tactische BIG staat is uitgevoerd. Hier wordt echter wel aan gewerkt. Een dergelijke baseline kan niet direct na invoering uitgevoerd worden. Hier moet tijd voor genomen worden. Het lijkt er wel op dat de gemeente Schijndel op de goede weg is, aangezien ze er actief mee bezig zijn.

Uit de enquête die is afgenomen bij de werknemers van de gemeente Schijndel blijkt dat een ruime meerderheid van de respondenten bekend is met het bestaan van het databeveiligingsbeleid. De bekendheid met de inhoud van dit beleid is echter een stuk lager. Slechts 12 procent van de respondenten geeft aan volledig bekend te zijn met de inhoud van het informatiebeveiligingsbeleid. Ondanks dat geeft een kleine meerderheid aan dat ze actief bezig zijn met databeveiliging. Slechts één vijfde van de ondervraagden geeft aan dat ze tevreden zijn met de manier waarop verwachtingen worden gecommuniceerd.

Binnen de gemeente Sint-Oedenrode blijkt dat nog niet alles wat in haar informatiebeveiligingsbeleid staat reeds wordt uitgevoerd. De gemeente Sint-Oedenrode heeft er bewust voor gekozen om de BIG van de IBD minimaal toe te passen omdat de fusie aanstaande is. Het beleid lijkt, in ieder geval tot de fusie, wel adequaat uitgevoerd te worden.

Uit de enquête die is afgenomen bij de werknemers van de gemeente Sint-Oedenrode blijkt dat bijna iedereen bekend is met het bestaan van het databeveiligingsbeleid. Ondanks dat geeft slechts 7 procent hiervan aan dat ze volledig weten wat er in het databeveiligingsbeleid staat. Meer dan 70 procent van de werknemers geeft echter aan dat ze actief bezig zijn met databeveiliging. Slechts één vijfde van de ondervraagden geeft aan dat ze tevreden zijn met de manier waarop verwachtingen worden gecommuniceerd.

Binnen de gemeente Veghel wordt nog niet alles wat in de Tactische BIG is opgenomen direct uitgevoerd. Het opstellen van dergelijke procedures kost immers tijd, en de Tactische Baseline is nog niet zo lang geleden ingevoerd. De gemeente Veghel is wel actief bezig met het opstellen van procedures, maar vanwege de fusie zal hier na de fusie verder aan gewerkt moeten worden.

De werknemers van de gemeente Veghel hebben aangegeven dat ze zich over het algemeen slechts gedeeltelijk bewust zijn van de inhoud van het informatie-beveiligingsbeleid, hoewel bijna iedereen weet dat dit beleid er is. Ondanks dat neemt de meerderheid van de werknemers wel maatregelen om data te beveiligen. De meerderheid is het erover eens dat verwachtingen duidelijker gecommuniceerd zouden moeten worden. Dit is dan ook een verbeterpunt voor de gemeente Veghel.

§5.2 Beantwoording centrale vraag

Dit onderzoek is gebaseerd op de centrale vraag: '*In hoeverre zijn het beleid, de processen en de protocollen met betrekking tot databeveiliging en datalekken van de gemeenten Schijndel, Sint-Oedenrode en Veghel juridisch correct en voldoende doelmatig om opgenomen te worden in het toekomstige beleid, de processen en de protocollen van de fusiegemeente Meierijstad, gelet op de geldende wet- en regelgeving omtrent privacy?*' Gebaseerd op de voorgaande hoofdstukken en de hierboven genoemde conclusies en aanbevelingen kan een definitief antwoord worden gegeven op deze vraag.

Het beleid, de processen en de protocollen met betrekking tot databeveiliging binnen de te fuseren gemeenten zijn, vanwege het feit dat ze gebaseerd zijn op de BIG van KING, allen rechtmatig. Tot op zekere hoogte zijn ze ook allemaal doelmatig, hoewel dat bij de gemeente Veghel iets meer het geval is dan bij de anderen. Bij het samenvoegen van de drie gemeenten kunnen het beleid van Schijndel, het beleid met betrekking tot databeveiliging van Sint-Oedenrode en het beleid van Veghel samengevoegd worden waarbij, zoals hierboven beschreven, gebruik gemaakt kan worden van de beste punten van deze gemeenten. Met betrekking tot databeveiliging is het beleid van de drie te fuseren gemeenten absoluut onrechtmatig. Geen van de drie gemeenten heeft een noemenswaardig beleid met betrekking tot het melden van datalekken aan de Autoriteit Persoonsgegevens en betrokkenen. Wanneer de fusie compleet is zal een dergelijk beleid dan ook moeten worden opgesteld.

De uitvoering van het beleid van de drie te fuseren gemeenten laat absoluut nog te wensen over. Hoewel hard gewerkt wordt om de uitvoering van het beleid te verbeteren weten veel werknemers niet goed wat van hen wordt verwacht.

§5.3 Aanbevelingen

§5.3.1 Beleid omtrent databeveiliging

Het huidige beleid van de drie gemeenten is rechtmatig en doelmatig genoeg om gebruikt te blijven worden tot de fusie op 1 januari 2017. Het is niet praktisch om voor een dergelijk korte periode nog stappen te ondernemen om deze te verbeteren.

Nadat de fusie is afgerond dient gekeken te worden hoe het beleid van de gemeente Meierijstad eruit moet komen te zien. Dit beleid, dat hoogstwaarschijnlijk eveneens gebaseerd zal zijn op de BIG van de IBD dient aangepast te worden naar de belangen van de gemeente Meierijstad. Voor deze aanpassingen wordt aangeraden om te kijken welke aanpassingen de drie te fuseren gemeenten op dit moment hebben doorgevoerd.

Geadviseerd wordt om de aanpassingen die de gemeente Schijndel heeft doorgevoerd niet door te voeren in de gemeente Meierijstad. Deze aanpassingen offeren veiligheid op voor gebruiksgemak, wat niet verstandig lijkt om door te zetten. Het gebruiksgemak wat hiermee gewonnen wordt valt immers in het niet tegenover de beveiligingsrisico's die deze met zich meebrengen.

De aanpassingen die de gemeente Sint-Oedenrode heeft gemaakt zouden deels aan te bevelen zijn. Het verwijderen van de specificaties die in de Tactische BIG van IBD staan is niet aan te raden. Deze specificaties geven immers verduidelijking en het verwijderen ervan voegt nauwelijks toe aan het gebruiksgemak. Het aanpassen van de BIG om beter te passen bij de gemeente waarvoor deze is aangepast, zoals de gemeente Sint-Oedenrode heeft gedaan, is wel aan te raden. De PDCA-cyclus die de gemeente Sint-Oedenrode gebruikt om haar beleid aan te toetsen is absoluut aan te raden en zorgt ervoor dat fouten in het beleid tijdig gelokaliseerd en opgelost kunnen worden. Deze hoeft echter niet noodzakelijk in het beleid zelf, zolang deze maar gebruikt wordt bij het uitvoeren van het beleid.

De aanpassingen die de gemeente Veghel heeft gemaakt zijn absoluut aan te bevelen. Alle aanpassingen die zijn gemaakt zijn erop gericht om de data zo goed mogelijk te beveiligen of het gebruiksgemak te verhogen. Bij de aanpassingen die zijn gemaakt voor gebruiksgemak is de (negatieve) impact die zij hebben op de beveiliging van data minimaal.

§5.3.2 Beleid omtrent de meldplicht datalekken

Met oog op de aanstaande fusie lijkt het onpraktisch om voor elk van de fuseren gemeenten een volledig beleid op te stellen omtrent het melden van datalekken. In plaats daarvan is aan te raden om een simpele procedure op te stellen voor het melden van datalekken, zodat het risico op een boete voor de fusie minimaal is. Een dergelijk beleid zou in ieder geval moeten specificeren wanneer een datalek gemeld dient te worden, wie een datalek moet melden en wat in een dergelijke melding opgenomen moet worden.

Wanneer de drie gemeenten daadwerkelijk gefuseerd zijn is het wel aan te raden om een volledig beleid op te stellen omtrent het melden van datalekken aan de Autoriteit Persoonsgegevens en eventuele betrokkenen.

Binnen een dergelijk beleid moeten in ieder geval de volgende stappen aan bod te komen: Na het ontdekken van een datalek dient allereerst een interne melding te worden gedaan. De procedure omtrent deze interne melding zou gebaseerd moeten zijn op de interne meldplicht datalekken van de gemeente Sint-Oedenrode[45], omdat dit de meest volledige van de drie is. Deze interne meldplicht moet als eerste uitgevoerd worden, zodat iedereen op de hoogte is van de te nemen stappen en hun rol daarin. Nadat deze stap is afgerond dient het datalek bestreden te worden. De manier waarop dit gebeurt is uiteraard afhankelijk van de situatie. Tegelijkertijd dient de impact van het datalek onderzocht te worden, zodat bepaald kan worden welke meldingen noodzakelijk zijn. Nadat hierop volgend de meldaanpak en de herstelaanpak zijn bepaald dient het datalek gemeld te worden en dienen er herstelwerkzaamheden uitgevoerd te worden. Ten slotte kan het volledige proces geëvalueerd worden.

Voor een uitgebreidere beschrijving van de te nemen stappen wordt aangeraden dat gebruik wordt gemaakt van het boek 'Grip op datalekken' van Hutter, Katus, Terstegge en Versmissen[46]. Dit boek bevat een volledige en uitgebreide beschrijving van alle acties die ondernomen moeten worden en door wie deze acties genomen moeten worden.

§5.3.3 Bewustzijn onder de werknemers

Aangezien het bewustzijn met betrekking tot de maatregelen omtrent het beveiliging van data vrij laag is wordt geadviseerd om er na de fusie meer aan te doen om ervoor te zorgen dat de werknemers weten wat van ze verwacht wordt. Uit de afgenomen enquêtes blijkt dat de werknemers zelf veel ideeën hebben over de manier waarop dit gecommuniceerd zou kunnen worden. Een trend die regelmatig terugkomt is dat de werknemers graag willen dat gecommuniceerd wordt wat de maatregelen specifiek voor hun betekenen. Het is dan ook aan te raden om na de fusie te proberen om een 'werknemersversie' van het databeveiligingsbeleid te maken. In deze werknemersversie dient duidelijk en beknopt in begrijpelijk taalgebruik te staan wat van de werknemers verwacht wordt.

Daarnaast wordt geadviseerd om de verwachtingen en vereisten op meerdere manieren onder de aandacht te brengen om de retentie te maximaliseren. Het is aan te raden om dit enerzijds digitaal te doen, bijvoorbeeld via intranet of e-mail, en anderzijds fysiek, door bijvoorbeeld het ophangen van posters en het geven van periodieke bijeenkomsten.

Naast deze maatregelen kunnen ook nog enkele andere maatregelen geadviseerd worden. Het gebruik van 'mystery guests' om de uitvoering van het beleid in de praktijk te controleren is hier een voorbeeld van. Dergelijke mystery guests zouden dan kunnen proberen om met werknemers naar binnen te lopen, zonder een sleutel nodig te hebben, en informatie te verzamelen. Ook kan een extern bedrijf ingehuurd worden om de uitvoering van het databeveiligingsbeleid onder de werknemers te toetsen.

[45] Tactische BIG Sint-Oedenrode, p. 40-41
[46] Hutter e.a. 2015

Literatuurlijst

Van Beelen e.a. 2015
D.C. van Beelen e.a., *Privacy en Gegevensbescherming*, Apeldoorn-Antwerpen: Maklu 2015.

Van Geenen 2015
A.D. van Geenen, *Een informatieveilige gemeente die ook nog "privacy-proof" is, kan dat? Nee, dat moet!* (notitie omtrent digitale gegevensverwerking), 2015.

Hutter e.a. 2015
J. Hutter e.a., *Grip op datalekken*, Deventer: Wolters Kluwer 2015.