Databeveiliging gemeente Etten-Leur

Eindrapportage

Oktober 2019

Postbus 5000
4700 KA ROOSENDAAL

www.rekenkamerwestbrabant.nl

rekenkamer WEST-BRABANT

Inhoudsopgave

1. Inleiding

In de huidige samenleving is databeveiliging een belangrijk onderwerp voor de gemeente. Dit wordt onderstreept door de resolutie die aangenomen is op de buitengewone ledenvergadering van de Vereniging van Nederlandse Gemeenten (VNG) eind 2013. In deze resolutie hebben alle gemeenten in Nederland zich uitgesproken databeveiliging bestuurlijk en organisatorisch in te bedden met als doel de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens te borgen. Hierbij is vastgelegd dat de Baseline Informatiebeveiliging voor Nederlandse gemeenten als standaard gebruikt wordt. Hiermee is databeveiliging transparant voor burgers, bedrijven en ketenpartners.

Daarnaast is de bescherming en beveiliging van persoonsgegevens onderworpen aan steeds strengere wet- en regelgeving. 25 mei vorig jaar is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze Europese wet is er op gericht dat elke organisatie die persoonsgegevens verwerkt, zoals iedere gemeente, dit op een deugdelijke en verantwoorde manier doet. Hierbij wordt verwacht dat organisaties aantoonbaar in control zijn op haar verwerkingen van persoonsgegevens. In Nederland houdt de Autoriteit Persoonsgegevens (AP) hier toezicht op, op straffe van mogelijke boetes.

De Rekenkamer West-Brabant voert namens de gemeenteraad Etten-Leur onderzoek uit naar databeveiliging. Daarbij worden zowel beleid als de uitvoering in de praktijk onderzocht. Niet alleen de 'harde' aspecten (processen en systemen) zijn van belang, maar ook de meer 'zachtere' aspecten (houding en gedrag). De uitvoering van dit onderzoek wordt gedaan door onderzoeksbureau BMC.

1.1. Beoordelen én leereffect

Het aspect 'leren' vormt een belangrijk element in de wijze waarop de rekenkamer West-Brabant onderzoeken benadert. Uiteraard gaat het bij een rekenkameronderzoek om het onderbouwd beoordelen van beleid, een initiatief of investering en het zichtbaar maken van tekortkomingen of juist het overtreffen van verwachtingen. Maar minstens zo belangrijk is het toevoegen van kennis en inzicht zodat de rollen van raad, het college en het ambtelijk management worden versterkt en handelingsperspectief beschikbaar komt om hier concreet aan te werken.

1.2. Centrale Onderzoeksvraag en deelvragen

De centrale onderzoeksvraag luidt:

Welk beleid heeft de gemeente Etten-Leur geformuleerd over databeveiliging en hoe wordt uitvoering aan dit beleid gegeven?

Daarbij worden twee onderwerpen onderscheiden waarlangs de onderzoeksvragen gerangschikt worden, te weten informatieveiligheid en privacy.

De centrale onderzoeksvraag is vervolgens uitgewerkt in deelvragen en een bijbehorend normenkader. Deze zijn opgenomen in bijlage 2.

Naast de oorspronkelijke deelvragen zijn *extra* deelvragen toegevoegd op verzoek van de gemeenteraad. Deze zijn:

1. Voldoet de gemeente Etten-Leur aan wet- en regelgeving aangaande de inzet van big data en data-analyse?

2. Is de ambtelijke organisatie voldoende toegerust (qua kennis en kunde) om, op een veilige manier en conform wet- en regelgeving, big data en data-analyse in te zetten?
3. Op welke wijze kan de gemeenteraad hier nog extra richting meegeven? Is er een handelingsperspectief te bedenken voor de gemeenteraad?
4. Hoe wordt in de digitale dienstverlening de afweging gemaakt tussen dataminimalisatie en het streven naar eenmalige gegevensuitvraag?
5. Hoe is in het sociaal domein geborgd dat in beleids- en uitvoeringsprocessen het gebruik en samenbrengen van persoonsgegevens verloopt volgens de landelijke en gemeentelijke richtlijnen?
6. Hoe kan de gemeenteraad haar kaderstellende en controlerende rol invullen?

1.3. Nota van Bevindingen: Objectief vastgelegde feiten

De Nota van Bevindingen bevat objectief vastgelegde feiten die tijdens het onderzoek verzameld zijn. Om te komen tot deze feiten is ontvangen documentatie (zie bijlage 1) bestudeerd en is informatie, opgehaald tijdens de interviews, gebruikt. Deze Nota van Bevindingen is voor wederhoor voorgelegd aan de ambtelijke organisatie.

Het onderzoek is ingedeeld in twee onderwerpen, te weten informatieveiligheid en privacy. Hiervoor zijn normenkaders samengesteld. Deze normenkaders zijn gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG) voor informatieveiligheid en de '10 stappen' van de Autoriteit Persoonsgegevens (AP) voor privacy[1]. Een groot deel van de normen is gelijk voor zowel het onderdeel informatieveiligheid als privacy. Voor de leesbaarheid zijn deze normen zoveel mogelijk samengevoegd. Daarnaast zijn er nog normen en onderdelen die alleen het onderwerp informatieveiligheid of het onderwerp privacy raken.

1.4. Doelmatigheid en Doeltreffendheid

In dit onderzoek is ook informatie verzameld om een uitspraak te kunnen doen over de doelmatigheid[2] en doeltreffendheid[3] van het beleid rond informatieveiligheid en privacy. Hiervoor wordt gebruik gemaakt van bestaande begrotingen, waarin kosten voor formatie, licentie en incidentele en projectmatige uitgaven zijn uitgewerkt. Tevens worden jaarplannen, voortgangsrapportages en besluiten naar aanleiding van deze rapportages betrokken bij de beoordeling van de doelmatigheid en doeltreffendheid. Daarnaast baseren we ons op onze kennis en ervaring rond het organiseren en bekostigen van informatiebeveiliging en privacy bij gemeenten van vergelijkbare omvang. De ervaring leert ons dat bij gemeenten van soortgelijke grootte (40.000 - 50.000 inwoners) gemiddeld ongeveer 2 FTE aanwezig is voor de invulling van de rollen van Security Officer, Privacy Officer en Functionaris Gegevensbescherming (FG)[4][5]. De verdeling van de inzet kan

[1] Organisatie geeft aan dat zij gebruik maakt van het normenkader van het Centrum voor Informatiebeveiliging en Privacy (CIP). Dit is ook een goed normenkader om informatiebeveiliging en privacy in te richten in de organisatie.
[2] Doelmatigheid: Of en zo ja in welke mate de voorbereiding, de organisatie en de uitvoering van het beleid efficiënt verlopen
[3] Doeltreffendheid: Of en zo ja, in welke mate de beoogde effecten van het beleid daadwerkelijk zijn behaald
[4] Dit is op basis van een vergelijking met vijf andere gemeenten.
[5] Benodigde FTE is afhankelijk van ambitieniveau, kennis en expertise van de personen die de rollen invullen en het reeds aanwezige niveau van informatieveiligheid en privacy.

verschillen, maar gemiddeld genomen is deze 0,5 - 1 FTE voor de Security Officer en voor de Privacy Officer 0,5 FTE, net als voor de FG. Deze cijfers zullen dan ook gebruikt worden bij de conclusies.

1.5. Leeswijzer

Deze Rapportage is als volgt opgebouwd.

Informatieveiligheid & Privacy

1. Beleid
2. Organisatie
3. Personele beveiliging & bewustwording
4. Beheer van beveiligingsincidenten
5. Naleving
6. Information Security Management System (ISMS) & Privacy Management System (PMS)

Informatieveiligheid

1. Beheer van bedrijfsmiddelen
2. Fysieke beveiliging
3. Beheer van communicatie- & bedienprocessen
4. Toegangsbeveiliging
5. Verwerking, ontwikkeling en onderhoud van informatiesystemen

Privacy

1. Rechten van betrokkenen
2. Register van verwerkingen
3. Data Protection Impact Assessment (DPIA)
4. Privacy-by-design
5. Verwerkersovereenkomsten

Extra onderzoeksgebieden

1. Gebruik Big Data en Data-analyse
2. Dataminimalisatie, eenmalige gegevensverstrekking en samenbrengen persoonsgegevens in klantprocessen (met name Sociaal Domein)
3. Kaderstellende en controlerende rol gemeenteraad
4. Casus: Automatisering gemeenteraad

2. Informatieveiligheid & Privacy

2.1. Beleid

Doel

Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging en privacy dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.

Norm

Er dienen een Informatiebeveiligingsbeleid en een privacybeleid aanwezig te zijn wat is goedgekeurd en uitgedragen door het hoogste management, vastgesteld door het college en bekendgemaakt bij de Raad.

Deelvragen

1. Is er informatieveiligheidsbeleid aanwezig dat gebaseerd is op de Baseline Informatiebeveiliging Gemeenten (BIG)?
2. Hoe is dit beleid tot stand gekomen en welke betrokkenheid hebben respectievelijk college en raad daarbij gehad?
3. Is er privacybeleid aanwezig?
4. Hoe is dit beleid tot stand gekomen en welke betrokkenheid hebben respectievelijk college en raad daarbij gehad?

Bevindingen

Er is een, door het college van B&W op 27 maart 2018 vastgesteld[6], informatieveiligheidsbeleid aanwezig. Dit beleid is gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG) en geldt tot 2020. Het informatieveiligheidsbeleid is regionaal (in de ICT Samenwerking ICTWBW[7]) ontwikkeld en hier en daar aangepast naar de lokale situatie. Het college van B&W is bij de totstandkoming van het beleid niet inhoudelijk betrokken. Het beleid is wel vastgesteld door het college.

Er is een organisatiebreed privacybeleid en -reglement aanwezig en vastgesteld door het college van B&W op 24 april 2018. De gemeente geeft aan dat het privacybeleid en –reglement op 24 april 2018 ter kennisname aan de gemeenteraad zijn aangeboden en dat hier geen reactie op gekomen is. Het beleid is gebaseerd op de Algemene Verordening Gegevensbescherming (AVG). Dit beleid is bewust op een praktische manier opgesteld in samenwerking met het MT en teamleiders, om privacy als onderwerp van de kant te krijgen. Op dit moment is het vooral een vertaling van het wettelijke kader AVG. Het beleid is vanuit de operatie ontwikkeld met inachtneming van de strategische doelstellingen van de organisatie. Er is geen sprake van een methodologische uitwerking vanuit de

[6] Zie voor (vastgestelde) documentatie bijlage 1
[7] ICT Samenwerking West-Brabant West is een bedrijfsvoeringsorganisatie op grond van de Wet gemeenschappelijke regelingen, ontstaan uit een samenwerking tussen de gemeenten Bergen op Zoom, Etten-Leur, Moerdijk, Roosendaal en Tholen. Sinds augustus 2015 is het ICT-beheer en ICT-onderhoud van de gemeenten en een aantal gemeenschappelijke regelingen hier ondergebracht.

strategische doelstellingen naar het privacybeleid. Het college van B&W is niet actief betrokken geweest bij de totstandkoming van het beleid. Het beleid is wel vastgesteld door het college en daarvoor besproken met de portefeuillehouder.

Naast dit organisatiebrede privacybeleid en -reglement is er een privacybeleid specifiek voor het Sociaal Domein aanwezig. Deze is specifiek opgesteld voor en toepasbaar op het Sociaal Domein. Het beleid is vastgesteld door het college van B&W op 8 januari 2019. Hieraan zitten nog twee privacyprotocollen gekoppeld, te weten voor Jeugdhulp en Maatschappelijke Ondersteuning. Deze set is tevens ter informatie aangeboden aan de gemeenteraad op 10 januari 2019.

In de Jaarrekening 2017 wordt een uitgebreide toelichting gegeven op het onderwerp 'Informatieveiligheid', als onderdeel van het hoofdstuk 'Bedrijfsvoering'. Een specificatie van structurele en incidentele investeringen is niet in de Jaarrekening opgenomen. In het college-besluit van 27 maart 2018, waarin het informatiebeleid wordt vastgesteld, is geen financiële paragraaf opgenomen. In het besluit wordt het MT verzocht "de beleidsmaatregelen waar nodig te vertalen in concrete keuzes en de implementatie hiervan in de bedrijfsvoering". In interviews met de ambtelijke organisatie is aangegeven dat structureel en geoormerkt budget voor informatieveiligheid ontbreekt en dat bekostiging hiervan op dit moment plaatsvindt uit andere bedrijfsvoeringsbudgetten.

Beantwoording deelvragen

1. Is er informatieveiligheidsbeleid aanwezig dat gebaseerd is op de Baseline Informatiebeveiliging Gemeenten (BIG)?
Ja, er is een informatieveiligheidsbeleid aanwezig dat gebaseerd is op de BIG, d.d. 27 maart 2018.

2. Hoe is dit beleid tot stand gekomen en welke betrokkenheid hebben respectievelijk college en raad daarbij gehad?
Het beleid is regionaal, met meerdere gemeenten, tot stand gekomen. Het college van B&W is bij de totstandkoming van het beleid niet inhoudelijk betrokken. Het beleid is wel vastgesteld door het college. De gemeenteraad is niet aanvullend geïnformeerd over dit beleid.

3. Is er privacybeleid aanwezig?
Ja, er is een organisatiebreed privacybeleid en -reglement aanwezig en vastgesteld door het college van B&W op 24 april 2018. De gemeente geeft aan dat het privacybeleid en –reglement op 24 april 2018 ter kennisname aan de gemeenteraad zijn aangeboden. Daarnaast zijn er nog een privacybeleid en specifieke protocollen aanwezig voor het Sociaal Domein. Deze hele set aan documenten is ter informatie aangeboden aan de gemeenteraad d.d. 10 januari 2019.

4. Hoe is dit beleid tot stand gekomen en welke betrokkenheid hebben respectievelijk college en raad daarbij gehad?
Ook voor het privacybeleid geldt dat het college van B&W niet inhoudelijk betrokken is geweest bij de totstandkoming van het beleid.

Conclusies

Er zijn zowel een informatieveiligheidsbeleid als een privacybeleid en –reglement aanwezig en vastgesteld door het college. Het college heeft geen actieve rol gehad in de totstandkoming zo ook de gemeenteraad niet. Het organisatiebrede privacybeleid en het privacybeleid en specifieke protocollen voor het Sociaal Domein zijn ter informatie aangeboden aan de gemeenteraad.

Er zijn geen structurele budgetten opgenomen voor het implementeren van beleidsmaatregelen rondom informatieveiligheid en privacy.

Risico's

Rol college

Door een weinig actieve rol van het college bij de totstandkoming van het beleid is het risico aanwezig dat informatieveiligheid en privacy onvoldoende aandacht krijgt op bestuurlijk niveau, waardoor sturing vanuit bestuur op de onderwerpen onvoldoende aandacht krijgt.

Structurele budgetten

Door geen structureel budget te alloceren voor implementatie van maatregelen rondom informatieveiligheid en privacy bestaat het risico dat maatregelen niet geïmplementeerd worden en het lastig is een hoger niveau van databeveiliging te bereiken.

Aanbevelingen

Betrek het college actief bij de totstandkoming van de komende beleidsstukken van informatieveiligheid en privacy. Alloceer, omwille van de implementatie van de beleidsmaatregelen, voldoende structurele budgetten voor zowel informatieveiligheid als privacy.

2.2. Organisatie

Doel

Beheren van de informatiebeveiliging en privacy binnen de organisatie.

Norm

De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor informatiebeveiliging en privacy worden toegekend en gecommuniceerd.

Deelvragen

1. Welke rollen en verantwoordelijkheden zijn beschreven op het vlak van informatieveiligheid?
2. Hoe worden deze rollen in de praktijk gebracht?
3. Welke rollen en verantwoordelijkheden zijn beschreven op het vlak van privacy?
4. Hoe worden deze rollen in de praktijk gebracht?

Bevindingen

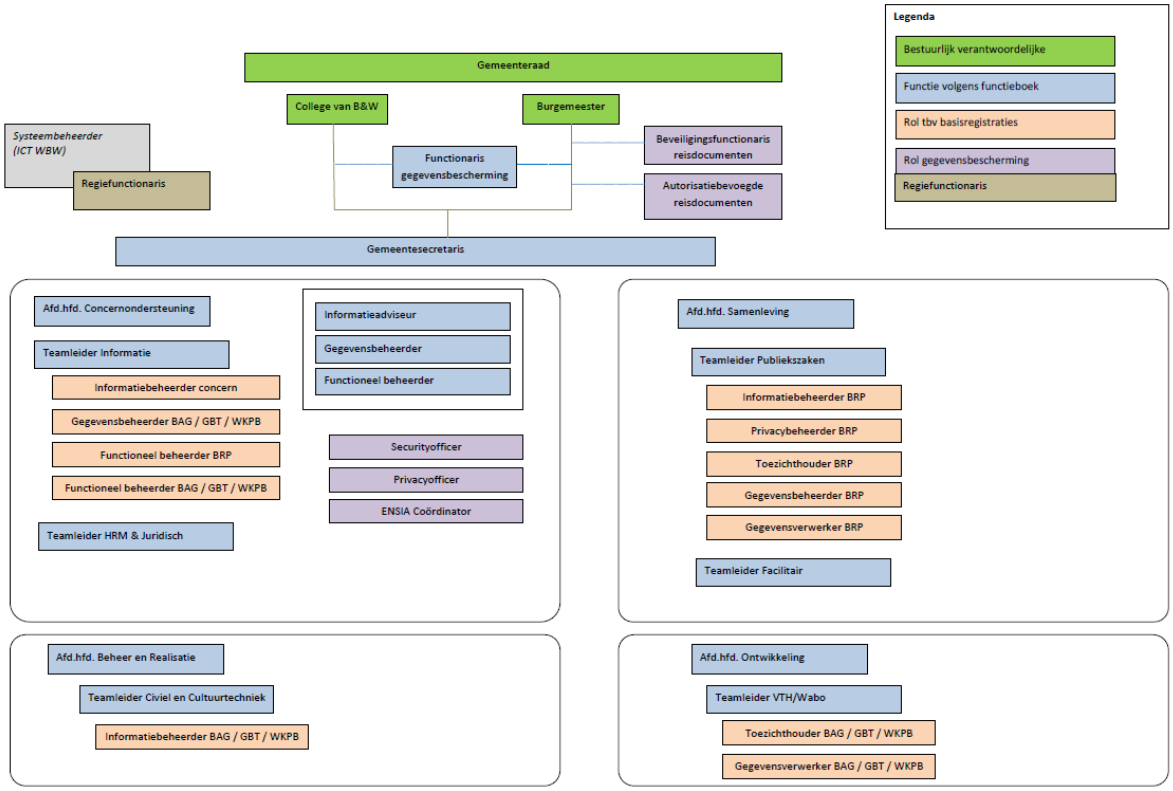
Het informatieveiligheidsbeleid bevat een aparte bijlage waarin rollen zijn uitgeschreven, de verantwoordelijkheden benoemd en de organisatie van informatieveiligheid en ook privacy wordt vormgegeven. De organisatie van informatiebeveiliging en privacy is nog niet aangepast aan HR21[8]. De Security Officer coördineert de informatieveiligheidswerkzaamheden. Voor de rollen van Security Officer en die van Privacy Officer zijn tijd en capaciteit gereserveerd in de functies van 'Informatieadviseur'. De Functionaris Gegevensbescherming is een formele functie in het functiehuis.

In het privacybeleid- en reglement is geen formele vastlegging van de rollen en verantwoordelijkheden in de organisatie aangetroffen. De rollen van Privacy Officer en Functionaris Gegevensbescherming (FG) zijn wel opgenomen en beschreven in het informatieveiligheidsbeleid. De rol van Privacy Officer is toegewezen aan een medewerker in de functie 'Informatieadviseur'. Daarnaast is een functie Functionaris Gegevensbescherming (FG) aanwezig en ingevuld en is deze medewerker officieel benoemd en aangemeld bij de Autoriteit Persoonsgegevens (AP), zoals wettelijk verplicht. De FG is daarbij een volledige functie. Voor de rol van Privacy Officer is, als gezegd, tijd en capaciteit gereserveerd in de functie 'informatieadviseur'.

Contact met afdelingen wordt zo toegankelijk mogelijk gemaakt, bijvoorbeeld door de inrichting van een speciaal e-mailadres. Verder worden afdelingen actief benaderd en opgezocht, door de drie genoemde rollen, om elkaar te leren kennen en te bespreken waar voor de afdelingen de pijn en risico's liggen. Op deze laagdrempelige manier wordt getracht de (redelijk) nieuwe onderwerpen informatieveiligheid en privacy bij alle afdelingen en medewerkers tussen de oren te brengen. De vervolgstap is om ambassadeurs in de afdelingen te benoemen en deze formeel in de organisatie op te nemen en de rollen en verantwoordelijkheden te benoemen.

[8] HR21 is het (nieuwe) functiewaarderingssysteem voor functiewaardering en -beschrijving voor gemeenten

In het Informatieveiligheidsbeleid is onderstaand organogram toegevoegd dat inzicht geeft in de verschillende functies, rollen en verantwoordelijkheden. Uitgangspunt hierbij is dat zowel informatieveiligheid als privacy een lijnverantwoordelijkheid is. Hierin is zichtbaar dat de Functionaris Gegevensbescherming (FG) is opgenomen in het functieboek. Deze is onderdeel van team control en heeft een onafhankelijke rol. De Security Officer, Privacy Officer en ENSIA coördinator zijn rollen die zijn toegekend aan bepaalde medewerkers (in de huidige situatie aan informatieadviseurs) als onderdeel van hun functie. Deze informatieadviseurs zijn onderdeel van het team Informatie[9]. Deze rollen zijn deze medewerkers toegewezen door het college van B&W door vaststelling van het informatieveiligheidsbeleid, d.d. 27 maart 2018.



Figuur 1: Organisatie van informatievoorziening van gemeente Etten-Leur (Informatiebeveiligingsbeleid 2017-2020, bijlage 1)

Beantwoording deelvragen

1. Welke rollen en verantwoordelijkheden zijn beschreven op het vlak van informatieveiligheid?

Er zijn verschillende rollen vastgelegd op het gebied van informatieveiligheid. Deze zijn vastgelegd in een aparte bijlage van het informatieveiligheidsbeleid.

[9] team Informatie is onderdeel van afdeling Concernondersteuning en bestaat uit 25 medewerkers die zich richten op de werkzaamheden in het i-domein (van Archief tot i-adviseur en van Security Officer tot Functioneel Beheerder)

2. Hoe worden deze rollen in de praktijk gebracht?
Alleen voor de rol van Security Officer & Privacy Officer is tijd en capaciteit in de functie van 'Informatieadviseur' belegd.

3. Welke rollen en verantwoordelijkheden zijn beschreven op het vlak van privacy?
In het privacybeleid zijn geen rollen en verantwoordelijkheden vastgelegd.

4. Hoe worden deze rollen in de praktijk gebracht?
Geconstateerd is dat de rollen Functionaris Gegevensbescherming en Privacy Officer wel aanwezig zijn, zonder de officiële vastlegging in het beleidsdocument. De Functionaris Gegevensbescherming betreft een functie die is opgenomen in het functiehuis. De rol van Privacy Officer is belegd in de functie van Informatieadviseur.

Conclusies

Rollen en verantwoordelijkheden voor informatieveiligheid en privacy zijn vastgelegd in het informatieveiligheidsbeleid. De rollen zijn verder niet vastgelegd in het privacybeleid. Geconcludeerd wordt dat alleen de Functionaris Gegevensbescherming een volwaardige functie is welke is opgenomen in het functieboek. Voor de rollen van Security Officer en Privacy Officer is tijd en capaciteit gereserveerd binnen hun functies, maar is niet aantoonbaar 0,5 – 1 FTE beschikbaar.
Als we dit vergelijken met de ervaring van de ingezette capaciteit bij gemeenten van vergelijkbare grootte (zie paragraaf 1.4) dan zien we dat de tijdsinzet voor zowel de Security Officer als de Privacy Officer aan de lage kant is. De gemiddelde capaciteit voor een Security Officer bij een vergelijkbare gemeente is 0,5 - 1 FTE en die voor de Privacy Officer 0,5 FTE.

Risico's

Onderzoekers constateren dat op operationeel niveau de juiste dingen gedaan en opgepakt worden binnen gemeente Etten-Leur om voor verplichtingen als audits en zelfevaluaties te slagen. Daarentegen zijn de onderwerpen nog onvoldoende verankerd op strategisch en tactisch niveau. Hierdoor bestaat het risico dat informatieveiligheid als onderwerp onvoldoende of te laat wordt meegenomen in strategische beleidsbeslissingen in bijvoorbeeld het sociaal domein of bij samenwerkingen.

Aanbevelingen

Zorg dat zowel de Security Officer als de Privacy Officer volwaardige functies worden, welke opgenomen zijn met taken en verantwoordelijkheden in het functieboek. Licht de huidige beschikbare capaciteit en middelen nog eens goed door. Houd daarbij rekening met het gegeven dat het coördinerende en adviserende functies zijn en dat de informatieveiligheid en privacy te allen tijde een lijnverantwoordelijkheid zijn.

2.3. Personele beveiliging & Bewustwording

Doel

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude, misbruik van faciliteiten en datalekken te verminderen.

Norm

Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoort te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.

Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.

Deelvragen

1. Hoe worden (nieuwe) medewerkers geattendeerd op beleidsregels uit het informatieveiligheidsbeleid?
2. Zijn er procedures aanwezig voor indienst-, uitdienst- en doorstroomprocessen?
3. Wordt periodiek aandacht besteed aan bewustwording over het onderwerp informatieveiligheid?
4. Wordt periodiek aandacht besteed aan bewustwording over het onderwerp privacy?

Bevindingen

Indienst- uitdienst- en doorstroomprocessen

Er is een procedure aanwezig voor het indienst- en uitdienst melden van medewerkers en het wijzigen van functies. Onderdeel hiervan zijn het aanvragen en toekennen van fysieke toegang en het aanvragen en toekennen van autorisaties voor systemen en applicaties. Ten tijde van de interviews werd nog gebruik gemaakt van Excel lijsten en was het proces nog niet geautomatiseerd. Inmiddels is vastgesteld dat dit proces is geautomatiseerd. Daarnaast is in het ambtelijk wederhoor aangegeven dat de procedure nog verder geoptimaliseerd wordt. Op sommige plekken in de organisatie wordt gebruik gemaakt van een autorisatiematrix om te bepalen welke autorisaties aan welke functie toegekend mogen worden, maar nog lang niet overal. Tevens zit er geen gestructureerde, periodieke toetsing op de actualiteit van de autorisatiematrix en autorisaties. In het ambtelijk wederhoor is aangegeven dat aan een verdere verbetering hiervan wordt gewerkt.

Inwerkprogramma

Er is geen vastomlijnd inwerkprogramma, waarvan bijvoorbeeld de beleidsregels van het informatieveiligheidsbeleid onderdeel zijn. Verantwoordelijkheid voor het attenderen op informatieveiligheid en de beleidsregels ligt bij de verantwoordelijk leidinggevende. In de ambtelijke reactie is aangegeven dat er op dit moment wordt gewerkt om

informatieveiligheid en privacy op te nemen in het introductieprogramma voor nieuwe medewerkers.

Bewustwording
Er is veel aandacht voor bewustwording op de onderwerpen informatieveiligheid en privacy. Dit uit zich in het aanbieden van e-learnings, films en het spelen van een spel en het plaatsen van intranetberichten. Medewerkers worden steeds meer centraal geattendeerd op het onderwerp informatieveiligheid. Er is een bewustwordingsplan/-strategie, maar deze is niet vastgelegd op papier. Er wordt op dit moment wel gewerkt aan een 'Jaarplan gegevensbescherming 2019', waarvan bewustwording een onderdeel is.

Beantwoording deelvragen

1. Hoe worden (nieuwe) medewerkers geattendeerd op beleidsregels uit het informatieveiligheidsbeleid?
Er is geen vastomlijnd inwerkprogramma, waarvan bijvoorbeeld de beleidsregels van het informatieveiligheidsbeleid onderdeel zijn. Verantwoordelijkheid voor het attenderen op informatieveiligheid en de beleidsregels ligt bij de verantwoordelijk leidinggevende.

2. Zijn er procedures aanwezig voor indienst-, uitdienst- en doorstroomprocessen?
Ja, Er is een procedure aanwezig voor het indienst- en uitdienst melden van medewerkers en het wijzigen van functies.

3. Wordt periodiek aandacht besteed aan bewustwording over het onderwerp informatieveiligheid?
Ja, er is veel aandacht voor bewustwording op het onderwerp informatieveiligheid. Dit uit zich in het aanbieden van e-learnings, films en het spelen van een spel en het plaatsen van intranetberichten. Medewerkers worden steeds meer centraal geattendeerd op het onderwerp informatieveiligheid.

4. Wordt periodiek aandacht besteed aan bewustwording over het onderwerp privacy?
Er wordt periodiek aandacht besteed aan bewustwording voor privacy, net als voor informatieveiligheid.

Conclusies

Er wordt veel aan bewustwording over de thema's informatieveiligheid en privacy gedaan door de organisatie. Vaak in een toegankelijke vorm als via e-learnings en films. De bewustwordingsactiviteiten hebben een vrijblijvend karakter voor medewerkers en deelname is dan ook niet verplicht. Inwerkprogramma's worden aan de afdelingen zelf over gelaten wat betekent dat er verschillen zitten in wat nieuwe medewerkers wel of niet meekrijgen over informatieveiligheid en privacy. De organisatie heeft aangegeven dat er op dit moment wordt gewerkt om informatieveiligheid en privacy op te nemen in het introductieprogramma voor nieuwe medewerkers.

Het indienst- en uitdienstproces is geautomatiseerd. Dit zal de komende periode getoetst moeten worden om te bezien of het proces werkt.

Risico's

De risico's van het niet planmatig oppakken van bewustwordingsactiviteiten voor de organisatie, maar zeker ook voor nieuwe medewerkers, is dat er geen regie gevoerd kan

worden op het niveau van kennis en bewustzijn van medewerkers. Diegenen die het een interessant onderwerp vinden zullen vaak aan de bewustwordingsactiviteiten deelnemen en diegenen die het minder interessant of zelfs onnodig vinden zullen niet op vrijwillige basis deelnemen. De uitkomst hiervan is dat de mensen die je graag wilt bereiken niet komen en diegenen die al op een bewuste manier met het onderwerp bezig zijn juist wel komen. Tevens is er moeilijk grip te houden op wat er op afdelingen wordt verteld en meegegeven over de onderwerpen aan nieuwe medewerkers. Hierdoor stagneert het werken aan een steeds hoger bewustzijns- en toepassingsniveau van 'informatieveiligheid' en 'privacy' in de organisatie.

Aanbevelingen

Maak een jaarlijkse planning voor bewustwordingsactiviteiten, leg deze schriftelijk vast en rapporteer over de voortgang. Hierin kan een plan opgenomen worden wie te bereiken, met welk doel en met welke activiteiten. Het advies is om hier structureel budget voor te reserveren, zodat er jaarlijks activiteiten ondernomen kunnen worden. Daarnaast is het van belang om nieuwe medewerkers te voorzien van de kennis, kunde en handvatten om in hun werkzaamheden informatieveiligheid en privacy aandacht te geven.

Evalueer binnen een half jaar het geautomatiseerde indienst- en uitdienstproces en stel waar nodig bij.

2.4. Beheer van beveiligingsincidenten & datalekken

Doel

Bewerkstelligen dat informatiebeveiligingsgebeurtenissen, zwakheden en datalekken die verband houden met informatiesystemen en persoonsinformatie zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen en aan wettelijke verplichtingen kan worden voldaan.

Norm

Informatiebeveiligingsgebeurtenissen en datalekken behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd en op een adequate wijze te worden behandeld en mogelijk gemeld bij de toezichthouder.

Deelvragen

1. Is er een proces voor het melden van informatieveiligheidsincidenten, worden deze vastgelegd en wordt erover gerapporteerd?
2. Is dit proces ook bekend bij medewerkers?
3. Is er een proces voor het melden van datalekken, worden deze vastgelegd en wordt er over gerapporteerd?
4. Is dit proces ook bekend bij medewerkers?

Bevindingen

Er is zowel een procedure voor het melden van beveiligingsincidenten als voor het melden van datalekken aanwezig. Deze procedures verwijzen naar elkaar. Beide procedures zijn vastgesteld door de Informatiebeheerder op 5 februari 2019. De verantwoordelijkheid voor de uitvoer van de procedure (het melden van incidenten en datalekken) ligt bij het

verantwoordelijk lijnmanagement. Incidenten en datalekken kunnen door medewerkers gemeld worden via het selfserviceportal, via de applicatie voor IT Service management (waar deze direct worden vastgelegd) of via de mail. Na deze melding onderzoekt het datalekteam, bestaande uit de Security Officer, de FG en de Privacy Officer, het incident en bepaalt de aard en impact van het incident. Afhankelijk van de aard van het beveiligingsincident wordt dit team uitgebreid met andere functionarissen. De Privacy Officer adviseert de verantwoordelijk manager over het al dan niet doen van een melding bij de Autoriteit Persoonsgegevens (AP). Het datalekteam maakt een verslag van het incident, en adviseert over de mogelijke te treffen maatregelen. De FG doet de melding bij de AP en de lijnmanager is, in het verlengde van zijn of haar rol, verantwoordelijk voor het treffen van de maatregelen.

In de procedures is opgenomen dat jaarlijks gerapporteerd wordt aan het management over incidenten en datalekken. Vastgesteld is dat op 1 maart 2019 gerapporteerd is over de (aantallen) beveiligingsincidenten over 2018. Hierin wordt benoemd hoeveel incidenten zijn aangemerkt als datalek, waardoor het een gecombineerde rapportage betreft. Er is niet apart gerapporteerd over de datalekken van 2018.

Dat er gemeld wordt geeft aan dat de procedures bekend zijn bij medewerkers. Hierover wordt gecommuniceerd in bewustwordingsacties en intranetberichten voor de organisatie. De drempel voor het melden is laag. Medewerkers worden aangemoedigd om te melden. Dit gebeurt door regelmatig persoonlijk contact van de Functionaris Gegevensbescherming, de Privacy Officer en de Security Officer met de medewerkers op afdelingen. Het bewustzijn bij medewerkers wanneer iets een incident of datalek is en hoe te handelen om deze te voorkomen, kan volgens de geïnterviewden nog verder vergroot worden. Daar wordt jaarlijks aan gewerkt door middel van bewustwordingsacties. Voor 2019 zijn deze acties vastgelegd in het ‘Gegevensbescherming Jaarplan 2019’ welke op moment van onderzoek in concept aanwezig was.

Beantwoording deelvragen

1. Is er een proces voor het melden van informatieveiligheidsincidenten, worden deze vastgelegd en wordt erover gerapporteerd?
Ja, er is een procedure voor het melden van beveiligingsincidenten aanwezig. De incidenten worden gemeld en daarmee direct vastgelegd in het Serviceportaal. Het datalekteam maakt een verslag (rapportage) van elke incident.
In de procedure is opgenomen dat jaarlijks gerapporteerd wordt aan het management over incidenten. Vastgesteld is dat op 1 maart 2019 gerapporteerd is over de (aantallen) beveiligingsincidenten over 2018
2. Is dit proces ook bekend bij medewerkers?
Doordat incidenten gemeld worden door medewerkers kan geconcludeerd worden dat de procedure bekend is. Hierover wordt gecommuniceerd in bewustwordingsactiviteiten en middels intranetberichten.
3. Is er een proces voor het melden van datalekken, worden deze vastgelegd en wordt er over gerapporteerd?
Ja, er is een procedure voor het melden van datalekken aanwezig. De datalekken worden gemeld en daarmee direct vastgelegd in het Serviceportaal. Het datalekteam maakt een verslag (rapportage) van elk datalek.
In de procedure is opgenomen dat jaarlijks gerapporteerd wordt aan het management over datalekken. Niet duidelijk is of nog apart is gerapporteerd over de datalekken van 2018.

4. Is dit proces ook bekend bij medewerkers?
Doordat datalekken gemeld worden door medewerkers kan geconcludeerd worden dat de procedure bekend is. Hierover wordt gecommuniceerd in bewustwordingsactiviteiten en middels intranetberichten.

Conclusies

Geconcludeerd wordt dat het proces voor het melden van beveiligingsincidenten en datalekken nageleefd wordt en werkt. Er wordt (jaarlijks) aan het verantwoordelijk management gerapporteerd over de incidenten en datalekken.

Risico's

Op dit punt zien de onderzoekers weinig overgebleven risico's.

Aanbevelingen

Er zijn derhalve dan ook geen aanbevelingen op dit punt.

2.5. Naleving

Doel

Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.

Norm

Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.

Deelvragen

1. Is er een intern controleplan aanwezig waarin ook informatieveiligheid is opgenomen?
2. Wordt er ook gerapporteerd over deze controles?
3. Is er een intern controleplan aanwezig waarin ook privacy is opgenomen?
4. Wordt er ook gerapporteerd over deze controles?

Bevindingen

Er zijn geen controleplannen aanwezig (en dus ook geen rapportages hierover) voor informatieveiligheid en/of privacy vanuit het team control. Er wordt op dit moment gewerkt aan een bredere blik bij control dan alleen financiën. Het doel is om meer business control te zijn dan alleen financiële control. Hiervoor is een visie ontwikkeld door de concerncontroller en gepresenteerd aan het MT, college en de gemeenteraad. De visie is niet officieel vastgesteld. Deze is nog niet omgezet in een concreet implementatieplan met aanverwante acties. Het is de bedoeling van Team Control dat Informatieveiligheid en privacy onderdeel worden van dit bredere business control concept. Naleving en toetsing op informatieveiligheid en privacy gebeurt op dit moment nog allemaal informeel.

Beantwoording deelvragen

1. Is er een intern controleplan aanwezig waarin ook informatieveiligheid is opgenomen?
Nee, er is geen intern controleplan aanwezig waar informatieveiligheid onderdeel van is.
2. Wordt er ook gerapporteerd over deze controles?
Er vinden wel rapportages plaats, bijvoorbeeld over incidenten en datalekken (zie paragraaf 2.4), maar aangezien er geen intern controleplan aanwezig is, vindt hier ook geen structurele rapportage over plaats.
3. Is er een intern controleplan aanwezig waarin ook privacy is opgenomen?
Nee, er is geen intern controleplan aanwezig waar privacy onderdeel van is.
4. Wordt er ook gerapporteerd over deze controles?
Ook hier geldt dat er geen structurele rapportage plaatsvindt over interne controles op basis van een intern controleplan.

Conclusies

Er wordt vanuit Control op dit moment nog geen formele toetsing uitgevoerd op aspecten van informatieveiligheid en privacy. Hierdoor wordt de Plan-Do-Check-Act cyclus als vastgelegd in het Informatiebeveiligingsbeleid niet geheel doorlopen en vindt er, op deze wijze, geen onafhankelijke toetsing plaats op het naleven van procedures en de effectiviteit van beveiligingsmaatregelen en ingerichte processen.

Risico's

Doordat er geen formele, onafhankelijke toetsing plaatsvindt, is het sturen op informatieveiligheid en privacy door de verantwoordelijken (gemeentesecretaris en MT) lastig. Onafhankelijke controles en audits geven vaak andere en nieuwe inzichten voor verantwoordelijken. Door deze inzichten kan een hoger beveiligingsniveau gehaald worden. Zonder toezicht en inzicht zal de lijnorganisatie doen wat het kan en wil op de onderwerpen informatieveiligheid en privacy, maar wordt het nog niet echt aangespoord om dat stapje extra te zetten op deze onderwerpen. Door dat stapje extra gaat het niveau van databeveiliging omhoog.

Aanbevelingen

Stel jaarlijks een controleplan voor informatieveiligheid en privacy vast. Dit kan onderdeel zijn van een breder controleplan. Laat onder verantwoordelijkheid van Team Control controles uitvoeren, rapporteer hierover aan het management en doe daarbij voorstellen voor verbeteringen. Op deze wijze kan het lijnmanagement een grotere verantwoordelijkheid nemen voor informatieveiligheid en privacy binnen de eigen processen en gaat het niveau van databeveiliging omhoog.

2.6. Information Security Management System (ISMS) & Privacy Management System (PMS)

Doel

Borging en beheersing van de informatieveiligheids- en privacy-activiteiten en het borgen van de Plan-Do-Check-Act (PDCA) cyclus.

Norm

Er dient een PDCA-cyclus ingericht te zijn, gedocumenteerd en in werking. Hierover dient te worden gerapporteerd aan de verantwoordelijken.

Deelvragen

1. Wordt periodiek gerapporteerd aan de verantwoordelijken, college en raad over het onderwerp informatieveiligheid?
2. Hoe vindt bijsturing van het beleid plaats?
3. Wordt periodiek gerapporteerd aan de verantwoordelijken, college en raad over het onderwerp privacy?
4. Hoe vindt bijsturing van het beleid plaats?

Bevindingen

Het Information Security Management System (ISMS) en het Privacy Management System (PMS) zijn systematieken voor de borging en beheersing van de informatieveiligheids- en privacy-activiteiten binnen een organisatie. Deze systematieken zijn gebaseerd op de Plan-Do-Check-Act-cyclus[10].

Plan is het vaststellen van doelstellingen
Do voer de geplande werkzaamheden uit om te komen tot de doelstellingen
Check Meet het resultaat aan de vastgestelde doelstellingen
Act Stel waar nodig de werkzaamheden bij

Plan

Er zijn een vastgesteld informatieveiligheidsbeleid en privacybeleid en -reglement aanwezig, zie onderdeel 'Beleid'. In het informatieveiligheidsbeleid is opgenomen dat deze iedere drie jaar wordt herzien of wanneer omstandigheden daar aanleiding toe geven. Voor het privacybeleid en –reglement geldt dat deze iedere vier jaar worden geëvalueerd en waar nodig worden herzien.

Voor informatieveiligheid is een 'Informatiebeveiligingsplan' aanwezig van 29 juni 2018. Hierin is een plan opgenomen voor het implementeren van maatregelen uit de Baseline Informatiebeveiliging Gemeenten (BIG) en daarmee uit het vastgestelde Informatiebeveiligingsbeleid. In dit plan is niet opgenomen wie verantwoordelijk is voor het uitvoeren van bepaalde acties. Het plan loopt tot augustus 2019. In 2018 is een gemeentebrede Privacy Impact Assessment uitgevoerd. Deze rapportage van 25 juli 2018 is aanwezig. Hierin zijn diverse aanbevelingen opgenomen voor de korte en middellange

[10] PDCA-cyclus ook bekend als de kwaliteitscirkel van Deming

termijn. Deze rapportage wordt gebruikt als privacyplan totdat een actuelere versie beschikbaar is.

Op het moment van onderzoek is een 'Jaarplan Gegevensbescherming 2019' in concept aanwezig. Hierin zijn, op basis van de '10 stappen' van de Autoriteit Persoonsgegevens, acties voor 2019 geformuleerd op het gebied van gegevensbescherming en privacy. In dit plan is niet opgenomen wie verantwoordelijk is voor het uitvoeren van bepaalde acties.

Do
Door de Security Officer en de Privacy Officer wordt uitvoering en sturing gegeven aan de beide jaarplannen. De onderzoekers hebben niet vast kunnen stellen hoe ver de implementatie op dit moment is. Over de uitvoering van de beide plannen heeft nog geen structurele, periodieke rapportage plaatsgevonden.

Check
Wij hebben niet vast kunnen stellen dat er controles hebben plaatsgevonden op de effectiviteit van de getroffen maatregelen.

Act
Wij hebben niet vast kunnen stellen dat op basis van de controles bijstelling heeft plaatsgevonden.

Beantwoording deelvragen

1. Wordt periodiek gerapporteerd aan de verantwoordelijken, college en raad over het onderwerp informatieveiligheid?
Er vindt op dit moment geen structurele rapportage plaats aan verantwoordelijken, college en raad over het onderwerp informatieveiligheid.
2. Hoe vindt bijsturing van het beleid plaats?
In het informatieveiligheidsbeleid is opgenomen dat het IB beleid elke drie jaar wordt herzien of dat deze wordt aangepast wanneer daar aanleiding toe is.
3. Wordt periodiek gerapporteerd aan de verantwoordelijken, college en raad over het onderwerp privacy?
Er vindt op dit moment geen structurele rapportage plaats aan verantwoordelijken, college en raad over het onderwerp privacy.
4. Hoe vindt bijsturing van het beleid plaats?
In het privacybeleid – en reglement is opgenomen dat deze iedere vier jaar wordt geëvalueerd en zo nodig wordt herzien.

Conclusies

Geconcludeerd wordt dat de organisatie veel aandacht heeft gegeven aan de 'plan' fase. Hierdoor hebben de onderwerpen informatieveiligheid en privacy een plek gekregen in beleid en in de organisatie. Voor het implementeren van het beleid (de do fase) zijn een informatieveiligheidsplan en een Jaarplan Gegevensbescherming 2019 aanwezig (ten tijde van onderzoek was deze laatste nog een concept). Hiermee is richting gegeven aan de implementatie van het vastgestelde beleid
Waar het nog aan ontbreekt, is een structurele verantwoording over de implementatie, de toetsing op de effectiviteit van getroffen maatregelen (check) en daarmee de bijstelling van implementatie (act).

Risico's

Door het ontbreken van de check en de act fase en het ontbreken van een structurele rapportagecyclus bestaat het risico dat de verantwoordelijke bestuurders niet voldoende informatie hebben om goed te (be)sturen. Dit maakt het voor de ambtelijke organisatie moeilijker om de juiste koers aan te houden. Doordat de check nog niet is ingericht is onvoldoende inzichtelijk of maatregelen het effect bereiken wat van tevoren beoogd wordt. Daarnaast kunnen deze inzichten een basis vormen om bij te sturen in de act-fase.

Aanbevelingen

Het wordt aanbevolen om een structurele rapportagecyclus in te richten, richting het ambtelijk management, het college B&W en de gemeenteraad. Op deze manier kan, wanneer nodig, op tijd bijgestuurd worden door verantwoordelijken. Dit geeft de ambtelijke organisatie meer houvast over de te volgen richting.
Net als in paragraaf 2.5 bevelen wij aan om jaarlijks een intern controleplan op te stellen waarvan informatieveiligheid en privacy onderdeel zijn. Op deze manier kan de effectiviteit van maatregelen getoetst worden en op basis van de uitkomsten bijgestuurd worden.

3. Informatieveiligheid

3.1. Beheer van bedrijfsmiddelen

Doel

Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

Norm

Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden. Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met informatievoorzieningen.

Deelvragen

1. Is er een overzicht aanwezig met in gebruik zijnde IT-voorzieningen?
2. Is er een proces ingericht om dit actueel te houden?

Bevindingen

Zowel de gemeente zelf als ICT WBW beschikt over overzichten welke IT-voorzieningen aanwezig zijn. De gemeente heeft onlangs gehele nieuwe werkplekken uitgerold. Bij deze exercitie is alle software in beeld gebracht, inclusief versies en data. Voor het beheer is een softwarepakket aangeschaft, ingericht en in gebruik. Een medewerker binnen team Informatie is verantwoordelijk voor de actualiteit hiervan en beheert dit overzicht.

Beantwoording deelvragen

1. Is er een overzicht aanwezig met in gebruik zijnde IT-voorzieningen?
Ja, zowel ICT WBW als de gemeentelijke organisatie zelf beschikt over overzichten van IT-voorzieningen.
2. Is er een proces ingericht om dit actueel te houden?
Ja, er is een proces aanwezig om deze actueel te houden. Er is een medewerker verantwoordelijk voor dit proces en deze beheert ook het overzicht van IT voorzieningen.

Conclusies

De organisatie heeft goed inzichtelijk welke IT voorzieningen zij in bezit heeft en weet dus wat zij moet beveiligen.

Risico's

Op dit onderdeel zien de onderzoekers op dit moment geen substantiële risico's.

Aanbevelingen

Er zijn geen aanvullende aanbevelingen nodig op dit punt.

3.2. Fysieke beveiliging

Doel

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.

Norm

Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.

Deelvraag

1. Welke fysieke maatregelen zijn er getroffen om data te beveiligen?

Bevindingen

Het verzamelen van de bevindingen voor de fysieke beveiliging heeft plaatsgevonden door fysiek een ronde door het Stadskantoor te maken samen met een medewerker van Facilitaire Zaken.

Zonering & autorisaties

Er is zonering aanwezig en toegang tot deze zones en ruimtes is mogelijk door middel van autorisaties. Uitgifte van autorisaties vindt plaats op basis van functies en bevoegdheden.

In het pand zijn ook externe partijen aanwezig zoals het Werkplein Hart van Brabant en Regio West-Brabant. Deze medewerkers hebben dezelfde autorisaties als medewerkers van de gemeente Etten-Leur.

Een werkinstructie schrijft voor dat bezoekers worden aangemeld en geregistreerd en dat zij een bezoekerspas krijgen met bepaalde autorisaties. De organisatie ziet hier nog ruimte voor verbetering.

Inbraak-, overval-, agressie- en brandbeveiliging

Er is inbraakalarm aanwezig. Er zijn inbraak- en glasbreuksensoren aanwezig.
Er zijn meerdere paniekknoppen aanwezig. Daarnaast is er een overvalknop.
Verder zijn er ook rookmelders en brandblusapparatuur aanwezig. Ook zijn er brandwerende deuren aanwezig welke dichtklappen bij brand.

Fysieke informatie

Tijdens het onderzoek zijn weinig onbewaakte papieren dossiers of documenten gesignaleerd. De organisatie ziet hier zelf nog ruimte voor verbetering. Er zijn afgesloten papierbakken aanwezig waar medewerkers hun papier in weg kunnen gooien. Deze worden op een veilige manier geleegd, afgevoerd en vernietigd.
Toegang tot de archieven is beperkt middels autorisaties. Medewerkers kunnen dossiers aanvragen via het team Documentaire Informatievoorziening (DIV).

Digitale informatie
Tijdens het onderzoek zijn geen onbeheerde, openstaande computers gezien. Medewerkers 'locken' hun pc als ze weg gaan. Wanneer dit niet het geval is lockt de pc automatisch na een aantal minuten. Op de begane grond is, op enkele plekken, folie tegen de ruiten geplaatst, zodat meekijken van buiten bemoeilijkt wordt.

Beantwoording deelvraag

1. Welke fysieke maatregelen zijn er getroffen om data te beveiligen?
Zie voor beantwoording van deze deelvraag de bevindingen hierboven.

Conclusies

De fysieke inspectie heeft geresulteerd in de conclusie dat een pas met autorisaties nodig is om je te bewegen in het gemeentehuis. Zonder pas kom je in principe niet verder dan de publieke ruimtes.
Externen partijen die in het pand situeren en bezoekers hebben ook autorisaties om zich door het gebouw te bewegen.

Interne afspraken als het 'locken' van de computer bij afwezigheid en het bureau opruimen worden goed nageleefd. Ook de inbraak-, brand- en agressiebeveiliging is op een goed niveau.

Risico's

Dat sommige externen zich door het pand kunnen bewegen met een pas met autorisaties brengt het risico met zich mee dat zij mogelijk toegang hebben tot ruimtes met informatie en gegevens waar zij geen toegang toe zouden moeten hebben. Dit brengt het risico van datalekken met zich mee.

Aanbevelingen

Geadviseerd wordt om te onderzoeken in hoeverre het mogelijk is om de externe partijen die in het gebouw gehuisvest zijn, alleen toegang te geven tot hun eigen gedeelten van het gebouw.

3.3. Beheer van Communicatie- en bedienprocessen

Doel

Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.

Norm

Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.

Bedieningsprocedures bevatten informatie over opstarten, afsluiten, back-up- en herstelacties, afhandelen van fouten, doorvoeren van wijzigingen, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging. Er zijn procedures voor de behandeling van digitale media die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging.

Deelvraag

1. Zijn er processen ingericht voor de beheersing van de IT-voorzieningen, volgens Information Technology Infrastructure Library (ITIL) of soortgelijk?

Bevindingen

Zowel de gemeentelijke organisatie als ICT WBW heeft zijn eigen procedures, zoveel mogelijk gebaseerd op ITIL[11]. De procedures en processen voor beide organisaties staan redelijk los van elkaar.

Er is bijvoorbeeld een 'procedure wijzigingsbeheer' aanwezig bij gemeente Etten-Leur. Deze procedure geldt niet voor applicaties die beheerd worden door ICT WBW. ICT WBW heeft weer eigen procedures voor wijzigingsbeheer. Bij wijzigingen toetst ICT WBW, middels de ingerichte Change Advisory Board (CAB), de impact van de wijzigingen in de eigen organisatie (ICT WBW), maar betrekt hier niet standaard iemand van de gemeentelijke organisatie bij. Hetzelfde geldt andersom van de gemeente richting ICT WBW.

Beantwoording deelvraag

1. Zijn er processen ingericht voor de beheersing van de IT-voorzieningen, volgens Information Technology Infrastructure Library (ITIL) of soortgelijk?
Ja, er zijn zowel bij de gemeente als bij ICT WBW procedures aanwezig welke gebaseerd zijn op ITIL. De procedures van beide organisaties sluiten niet altijd goed op elkaar aan.

Conclusies

De processen en procedures van ICT WBW en de gemeentelijke organisatie sluiten niet altijd goed op elkaar aan, doordat beide organisatie hun eigen procedures en processen hanteren.

[11] ITIL zijn internationaal erkende standaarden hoe een IT dienstverlener haar processen het beste kan inrichten om het meest optimaal te garanderen dat haar klanten de producten en diensten ontvangen die zij wensen.

Risico's

Risico is dat beide organisaties langs elkaar heen werken en bijvoorbeeld wijzigingen doorvoeren die voor de andere organisatie van (negatieve) invloed is, zonder dat daarover van tevoren afstemming heeft plaatsgevonden.

Aanbevelingen

Aanbevolen wordt om de processen zoveel mogelijk op elkaar aan te laten sluiten en processen en procedures in gezamenlijkheid te ontwikkelen en toe te passen.

3.4. Toegangsbeveiliging

Doel

Beheersen van de toegang tot informatie.

Norm

Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van organisatie-eisen en beveiligingseisen voor toegang.

Deelvraag

1. Zijn er processen ingericht voor het toekennen en intrekken van toegangsrechten?

Bevindingen

Er is onlangs (in de onderzoeksperiode) een nieuw proces ingericht voor het toekennen en intrekken van toegangsrechten. Dit proces loopt via het selfserviceportal, welke is gekoppeld met het IT Service Management systeem van ICT WBW. De leidinggevende is verantwoordelijk voor het aanmelden van een nieuwe medewerker. Een medewerker krijgt slechts toegang tot een beperkte set aan (kantoor)applicaties. Wanneer voor de uitoefening van de werkzaamheden extra (domein specifieke) applicaties nodig zijn moet dit, door betreffende leidinggevende, worden aangevraagd en deze moet akkoord bevonden worden door de betreffende applicatie-eigenaar, voordat die rechten toegekend worden. De mogelijkheid om toegangsrechten toe te kennen op basis van "dezelfde rechten als medewerker X' is verleden tijd. De organisatie geeft in het ambtelijk wederhoor aan dat een procedure met een autorisatiematrix voor de gehele organisatie nog moet worden geïmplementeerd.

Intrekken van autorisaties gebeurt automatisch bij een tijdelijk contract wanneer het contract ten einde is. Anders is leidinggevende verantwoordelijk dat dit gemeld wordt. Hierop vindt controle plaats, maar dit is niet planmatig ingebed.

Beantwoording deelvraag

1. Zijn er processen ingericht voor het toekennen en intrekken van toegangsrechten?
Ja. Onlangs is er een nieuw proces ingericht voor het toekennen en intrekken van toegangsrechten.

Conclusies

Er is aandacht voor het goed inrichten van het indienst- en uitdienstproces met het toekennen van toegangsrechten. Er is een nieuw, geautomatiseerd proces ingericht waarvan de komende periode bekeken moet worden of dit (beter) werkt. In het proces is nog geen planmatige toetsing ingebed.

Risico's

Risico's wanneer dit proces niet goed ingericht is, is dat medewerkers te ruime autorisaties hebben en gegevens kunnen inzien welke zij voor de uitoefening van hun werkzaamheden niet nodig hebben. Dit kan leiden tot het niet voldoen aan wet- en regelgeving en datalekken. Het niet inbedden van een planmatige toetsing kan leiden tot verouderde autorisatiematrices en te ruim toegekende autorisaties.

Aanbevelingen

Aanbevolen wordt om na een bepaalde periode, bijvoorbeeld drie maanden, het nieuwe proces te evalueren en bij te sturen waar nodig. Richt daarnaast een planmatige toetsing op uitgegeven autorisaties en op de vastgestelde autorisatiematrices in en rapporteer hierover en stuur zo nodig bij.

3.5. Verwerking, ontwikkeling en onderhoud van informatiesystemen

Doel

Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

Norm

In eisen die vanuit de organisatie gesteld worden aan inkoop, gebouwaanpassingen, procesaanpassingen, nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.

Deelvragen

1. Op welke wijze wordt informatieveiligheid meegenomen in aanbestedings- en inkooptrajecten?
2. Hoe wordt regie gevoerd op de ICT-activiteiten bij de samenwerkingsorganisatie?

Bevindingen

Afdelingen kunnen zelf inkoop- en aanbestedingstrajecten in gang zetten. Hiervoor zijn zij niet altijd verplicht om het Inkoopbureau[12] in te schakelen. Ook zijn zij niet verplicht om team Informatie in te schakelen (bij aanschaf van IT faciliteiten). Wanneer team Informatie wordt ingeschakeld wordt gekeken naar privacy en informatieveiligheid, aangezien de Privacy Officer en de Security Officer in team Informatie zijn ondergebracht. Dit proces is niet formeel verankerd.

[12] Inkoopbureau West-Brabant is een samenwerkingsverband tussen gemeenten in de regio Zuid-West Nederland op het gebied van inkoop & aanbestedingen

Wanneer team Informatie niet wordt ingeschakeld is het afhankelijk van de afdeling zelf of privacy en informatieveiligheid worden meegenomen/afgewogen. Het maakt geen formeel onderdeel uit van de inkoopprocessen.

Er is met ICT West-Brabant West een Dienstverleningsovereenkomst afgesloten. Hierin staan de afspraken over producten, diensten, kwaliteit en financiën beschreven. Ook staat hierin beschreven dat er ieder kwartaal door ICT WBW wordt gerapporteerd. Tevens wordt er door ICT WBW een jaarverslag uitgebracht. Er is een Product Diensten catalogus (PDC) en een Service Level Agreement (SLA) aanwezig.

Maandelijks wordt een rapportage uitgebracht over de naleving van de SLA door ICT WBW. Ieder kwartaal vindt een rapportage en gesprek plaats over de naleving van de dienstverleningsovereenkomst. Deze landen in de Planning & Control documentatie binnen de organisatie.

Beantwoording deelvragen

1. Op welke wijze wordt informatieveiligheid meegenomen in aanbestedings- en inkooptrajecten?
Er is geen formeel verankerd proces voor inkoop- en aanbesteding waarin informatieveiligheid is meegenomen. Informatieveiligheid wordt meegenomen wanneer het team Informatie wordt ingeschakeld bij het traject.
2. Hoe wordt regie gevoerd op de ICT-activiteiten bij de samenwerkingsorganisatie?
Op ICT WBW wordt door middel van meerdere rapportagelijnen regie gevoerd.

Conclusies

Het is geen onderdeel van de inkoop- en aanbestedingsprocessen om informatieveiligheid en privacy een plek te geven. Dit betekent dat informatieveiligheid en privacy niet altijd onderdeel zijn van inkooptrajecten.

Op ICT WBW wordt door middel van meerdere rapportagelijnen regie gevoerd.

Risico's

Doordat informatieveiligheid en privacy geen formeel onderdeel zijn van de inkoop- en aanbestedingstrajecten loopt de organisatie het risico dat onvoldoende wordt nagedacht over deze aspecten bij de aankoop van bijvoorbeeld informatiesystemen. Hiermee wordt dan ook geen invulling gegeven aan security- & privacy-by-design[13]. Tevens is het zeer de vraag of de risico's die gelopen worden op het gebied van informatieveiligheid en privacy voldoende in beeld worden gebracht bij aankoop van systemen.

Aanbevelingen

Aanbevolen wordt om informatieveiligheid en privacy vast onderdeel te laten zijn van inkoop- en aanbestedingstrajecten. Hiermee wordt aan de voorkant invulling gegeven aan systematieken als security- & privacy-by-design.

[13] Security- & privacy-by-design betekenen dat je tijdens het ontwerp van een nieuwe applicatie, ict-omgeving of bij de start van een nieuw project rekening houdt met de beveiliging (van persoonsgegevens)

4. Privacy

4.1. Rechten van Betrokkenen

Doel

Bewerkstelligen dat de rechten van betrokkenen worden gewaarborgd conform wet- en regelgeving.

Norm

Er behoort een proces ingericht te zijn waar inwoners hun rechten rondom hun persoonsgegevens kunnen uitoefenen.

Deelvraag

1. Is er een proces ingericht en is dit ook bekendgemaakt bij medewerkers omtrent de rechten van betrokkenen (inzagerecht, recht op verwijdering)?

Bevindingen

Er is een procedure aanwezig omtrent de rechten van betrokkenen van 5 februari 2019. Hierin worden de verantwoordelijkheden en de processen beschreven hoe om te gaan met verschillende verzoeken van inwoners omtrent hun persoonsgegevens. Deze procedure is opgesteld op basis van de verplichtingen voortkomend uit de Algemene Verordening Gegevensbescherming (AVG).

De mogelijke verzoeken van burgers komen bij de Privacy Officer binnen. Hij heeft de procedure (mede) opgesteld en is verantwoordelijk voor de actualisatie hiervan. Wanneer een verzoek binnenkomt, stuurt de Privacy Officer dat aan en neemt afdelingen en teams mee in het proces. Door de sturing door de Privacy Officer worden medewerkers meegenomen in en bekend gemaakt met het proces en daarmee geldende procedures.

Beantwoording deelvraag

1. Is er een proces ingericht en is dit ook bekendgemaakt bij medewerkers omtrent de rechten van betrokkenen (inzagerecht, recht op verwijdering)?
Ja, er is een procedure aanwezig omtrent de rechten van betrokkenen, d.d. 5 februari 2019. De medewerkers worden, wanneer een verzoek binnenkomt, aangestuurd door de Privacy Officer en op die manier worden zij bekend gemaakt met de procedure.

Conclusies

Geconcludeerd wordt dat er een gedegen procedure is wanneer een inwoner zijn of haar rechten conform de AVG inroept, zoals recht van inzage.

Risico's

Wanneer dit proces niet goed is ingericht of de procedure niet goed wordt nageleefd kan dit leiden tot opgelegde dwangsommen.

Aanbevelingen

Het proces wordt niet dagelijks doorlopen, maar zeer sporadisch wanneer een inwoner zijn recht aanroept. Evalueer het proces na elke keer dat deze is doorlopen om zo verbeteringen door te kunnen voeren in dit proces.

4.2. Register van verwerkingen

Doel

Inzichtelijk hebben en actueel houden van verwerkingen van persoonsgegevens binnen de organisatie.

Norm

Er behoort een actueel overzicht te zijn waar de organisatie persoonsgegevens verwerkt, inclusief (wettelijke) grondslag. Ook dient een proces ingericht te zijn voor periodieke actualisatie van dit overzicht.

Deelvragen

1. Is er een actueel overzicht van verwerkingen aanwezig?
2. Op welke wijze wordt de actualiteit hiervan geborgd?

Bevindingen

Er is een Register van Verwerkingen aanwezig van de gehele organisatie. De verantwoordelijkheid voor de actualiteit van dit register ligt bij de afdelingen. Het Register is opgezet in 'Excel'. Inmiddels is het register ingevoerd in het Privacy Management Systeem (PMS), een speciale applicatie hiervoor. Het is de verantwoordelijkheid van de afdelingen zelf om wijzigingen aan het register tijdig door te geven aan de Privacy Officer en/of Functionaris Gegevensbescherming (FG).

De FG bewaakt de actualiteit van het register en toetst deze periodiek. Afdelingen moeten zich nog bewuster worden van deze verplichting en verantwoordelijkheid die zij daarbij hebben.

Beantwoording deelvragen

1. Is er een actueel overzicht van verwerkingen aanwezig?
Ja, er is een actueel overzicht van verwerkingen aanwezig.
2. Op welke wijze wordt de actualiteit hiervan geborgd?
Afdelingen zijn zelf verantwoordelijk voor de actualiteit van het overzicht. De FG toetst periodiek de actualiteit.

Conclusies

Er is een Register van Verwerkingen aanwezig, welke wordt bijgehouden in een speciale applicatie, het Privacy Management Systeem (PMS). De verantwoordelijkheid voor de actualiteit ligt bij de afdelingen. De FG toetst periodiek de actualiteit van het Register..

Risico's

Niet gevulde of het niet actueel zijn van het register kan leiden tot onderzoeken van de Autoriteit Persoonsgegevens (AP) en mogelijk tot boetes van diezelfde Autoriteit, omdat daarmee niet voldaan wordt aan wet- en regelgeving.

Aanbevelingen

Maak actualisatie van het register onderdeel van een cyclus en van resultaatverplichtingen van de afdelingen. Laat vanuit Team Control, mogelijk door de FG, de onafhankelijke toets plaatsvinden op actualiteit van het register.

4.3. Privacy Impact Assessment (PIA)

Doel

Bepalen en beheersen van risico's bij verwerkingen van persoonsgegevens.

Norm

Er is een proces ingericht voor het uitvoeren van Privacy Impact Assessments (PIA's).

Deelvragen

1. Is er een procedure aanwezig voor het uitvoeren van Privacy Impact Assessments (PIA's), worden deze geregistreerd en wordt er ook opvolging aan gegeven?
2. Is dit proces bekend bij de organisatie?

Bevindingen

Een Privacy Impact Assessment is een instrument om voorafgaand aan een project, de inrichting van een proces of de aankoop van een applicatie, privacy risico's in kaart te brengen om daarna maatregelen te treffen om deze risico's in te perken. Er is binnen gemeente Etten-Leur geen vaste procedure voor het uitvoeren van een PIA aanwezig. Wel zijn er informele afspraken die bij het inkopen van bijvoorbeeld informatiesystemen (software) het uitvoeren van een PIA verplichten. De inkopende afdeling is hier zelf verantwoordelijk voor. Dit gebeurt niet altijd, omdat afdelingen zich niet altijd bewust zijn dat dit een verplichting is.

Wanneer een PIA uitgevoerd wordt door de afdeling, gebeurt dit met behulp van het door de Functionaris Gegevensbescherming gekozen formulier. Dit formulier is ontwikkeld op basis van de 'Handleiding checklist PIA' van de Informatiebeveiligingsdienst (IBD), onderdeel van VNG Realisatie[14]. De FG en de Privacy Officer worden dan ook betrokken bij dit proces.

Beantwoording deelvragen

1. Is er een procedure aanwezig voor het uitvoeren van Privacy Impact Assessments (PIA's), worden deze geregistreerd en wordt er ook opvolging aan gegeven?
Er is geen vaste procedure aanwezig voor het uitvoeren van PIA's.

[14] VNG Realisatie is onderdeel van Vereniging voor Nederlandse Gemeenten (VNG). VNG Realisatie werkt samen met gemeenten aan (IT) oplossingen die de gemeentelijke uitvoering verbeteren.

2. Is dit proces bekend bij de organisatie?
Nee, want er is geen vast proces aanwezig.

Conclusies

Doordat een vaste procedure ontbreekt voor het uitvoeren van een PIA, wordt het uitvoeren van een PIA vaak vergeten.

Risico's

De risico's van het niet uitvoeren van een PIA is dat onvoldoende in beeld wordt gebracht welke risico's de organisatie loopt in een bepaald proces of bij een bepaald systeem op het gebied van privacy. Hierdoor is het mogelijk dat er onvoldoende maatregelen genomen worden die de privacy van inwoners in dat project, proces of informatiesysteem borgt. Dit vergroot de kans op datalekken en mogelijke boetes.

Aanbevelingen

Borg het uitvoeren van een PIA bij het opstarten van projecten, inkoop- en aanbestedingstrajecten en bij herinrichting van processen. Op deze wijze wordt privacy onderdeel van dit soort processen en wordt daarmee invulling gegeven aan het privacy-by-design principe.

4.4. Privacy-by-design

Doel

Borgen van de beveiliging van persoonsgegevens bij het inrichten of wijzigen van organisatieonderdelen, (IT-)faciliteiten of processen.

Norm

Privacy behoort onderdeel te zijn van aanbestedingen (inclusief het afsluiten van verwerkersovereenkomsten) en projecten.

Deelvragen

1. Op welke wijze wordt privacy meegenomen in aanbestedings- en inkooptrajecten?
2. Op welke wijze wordt de privacy geborgd binnen projectopdrachten?

Bevindingen

Er is geen vast aanbestedings- en inkooptraject waar privacy onderdeel van is. Budgetten voor aanschaf van bijvoorbeeld informatiesystemen (software) zijn decentraal bij afdelingen ondergebracht. Afdelingen zijn zelf verantwoordelijk voor de inkooptrajecten. Soms wordt het team Informatie betrokken, maar niet altijd. Bij team Informatie (waar de Privacy Officer deel van uitmaakt) wordt privacy meegenomen in de afwegingen bij aanschaffen van software en zo nodig en mogelijk meegenomen in bijvoorbeeld het Programma van Eisen. Wanneer afdelingen zelf het inkooptraject doen en team Informatie hier niet bij betrekken is privacy vaak geen onderdeel van het traject.

Voor de uitvoering van projecten geldt hetzelfde. Er is geen vast projectformulier of -proces waar privacy onderdeel van is. Bij projecten binnen team Informatie wordt dit wel vaak meegenomen. De Privacy Officer en de Security Officer zijn onderdeel van het team

Informatie. De lijnen binnen het team zijn kort, waardoor de Privacy Officer en Security Officer sneller betrokken worden bij projecten. Hier is het tevens afhankelijk van persoonlijk contact en korte lijnen, aangezien ook hier geen vast format aanwezig is voor projecten waar privacy onderdeel van uitmaakt.

Beantwoording deelvragen

1. Op welke wijze wordt privacy meegenomen in aanbestedings- en inkooptrajecten?
Er is geen formeel verankerd proces voor inkoop- en aanbesteding waarin privacy is meegenomen. Privacy wordt meegenomen wanneer het team Informatie wordt ingeschakeld bij het traject.
2. Op welke wijze wordt de privacy geborgd binnen projectopdrachten?
Dit geldt ook voor het uitvoeren van projecten.

Conclusies

Privacy is geen vast onderdeel van projectformulieren en inkoop- en aanbestedingstrajecten.

Risico's

Risico van het gegeven dat privacy geen vast onderdeel is van projectformulieren en inkoop- en aanbestedingstrajecten is dat privacy niet altijd of onvoldoende aandacht krijgt bij het starten van projecten en inkoop- en aanbestedingstrajecten. Hierdoor kan het zijn dat niet aan wet- en regelgeving wordt voldaan, wanneer bijvoorbeeld geen verwerkersovereenkomsten met leveranciers worden gesloten of bijvoorbeeld te ruime persoonsgegevens gedeeld worden tijdens projecten.

Aanbevelingen

Maak privacy onderdeel van standaard projectformulieren en van inkoop- en aanbestedingsprocessen en – documenten.

4.5. Verwerkersovereenkomsten

Doel

Beheersen van verwerking van persoonsgegevens door derde partijen.

Norm

Er behoren verwerkersovereenkomsten afgesloten te worden met zogenaamde verwerkers en deze dienen te zijn geregistreerd.

Deelvragen

1. Is er een actueel overzicht van verwerkers en verwerkersovereenkomsten aanwezig?
2. Is er een procedure voor het afsluiten van verwerkersovereenkomsten aanwezig en bekend bij de organisatie?

Bevindingen

Wanneer derde partijen voor de gemeente Etten-Leur persoonsgegevens verwerken (opslaan, wijzigen, verwijderen, inzien) stelt de AVG het afsluiten van een verwerkersovereenkomst verplicht. In zo'n verwerkersovereenkomst staan afspraken over hoe de derde partij de bescherming van de persoonsgegevens garandeert.
Binnen de gemeente ligt de verantwoordelijkheid voor het afsluiten en voor beheren van de (overzichten van) verwerkersovereenkomsten bij de lijnorganisatie. Er heeft onlangs een inventarisatie plaatsgevonden van de afgesloten verwerkersovereenkomsten. Hieruit is naar voren gekomen dat veel benodigde verwerkersovereenkomsten nog niet zijn afgesloten. De FG en Privacy Officer geven aan te sturen op het afsluiten van verwerkersovereenkomsten, door afdelingen, conform het model verwerkersovereenkomst van de Vereniging Nederlandse Gemeenten (VNG). Onderzoekers hebben geen rapportage over de inventarisatie aan verantwoordelijk management aangetroffen. Er is geen plan aangetroffen waarin het afsluiten van verwerkersovereenkomsten onderdeel is en waar beschreven is wie de verantwoordelijken zijn.

Er is geen vaste procedure voor het afsluiten van verwerkersovereenkomsten. Het is de bedoeling dat deze afgesloten worden tijdens het aanbestedings- of inkooptraject. Inkooptrajecten zijn decentraal ingericht, wat betekent dat de afdelingen hun eigen budgetten beheren en dus ook eigen inkooptrajecten starten. Daarbij wordt niet altijd gedacht aan het afsluiten van een verwerkersovereenkomst. Wanneer de software dan bij ICT wordt aangemeld moet er achteraf alsnog een verwerkersovereenkomst afgesloten worden.

Beantwoording deelvragen

1. Is er een actueel overzicht van verwerkers en verwerkersovereenkomsten aanwezig?
Onlangs is een inventarisatie gedaan naar de afgesloten verwerkersovereenkomsten. Daarmee is een overzicht van verwerkers en verwerkersovereenkomsten aanwezig.
2. Is er een procedure voor het afsluiten van verwerkersovereenkomsten aanwezig en bekend bij de organisatie?
Nee, er is geen vaste procedure aanwezig voor het afsluiten van verwerkersovereenkomsten.

Conclusies

Afdelingen kunnen hun eigen inkooptrajecten starten en daarbij wordt privacy en dus verwerkersovereenkomsten niet altijd in meegenomen. Het afsluiten van verwerkersovereenkomsten is geen vast onderdeel van aanbestedingstrajecten die vanuit het Inkoopbureau gefaciliteerd worden.

Risico's

Het niet formeel vastleggen in processen van het afsluiten van verwerkersovereenkomsten brengt het risico met zich mee dat deze verwerkersovereenkomsten niet worden afgesloten, waarmee niet wordt voldaan aan wet- en regelgeving. Dit kan boetes tot gevolg hebben. Tevens zijn er geen formele afspraken met een derde partij vastgelegd over hoe zij om moeten gaan met de persoonsgegevens van de inwoners van de gemeente, wanneer geen verwerkersovereenkomst is afgesloten.

Aanbevelingen

Maak het afsluiten van verwerkersovereenkomsten een vast onderdeel van alle inkoop- en aanbestedingstrajecten. Voer periodiek controles uit of verwerkersovereenkomsten zijn afgesloten.

5. Extra aandachtsgebieden

Deze extra aandachtsgebieden komen voort uit het gesprek met afgevaardigden van de gemeenteraad d.d. 20 november 2018, over het onderzoek naar Databeveiliging. Doel van dit gesprek was het informeren van de gemeenteraad van de gemeente Etten-Leur over de aanpak van het rekenkameronderzoek. De afgevaardigden van de fracties van de gemeenteraad hebben bovendien de onderzoekers voorzien van enkele vragen en onderwerpen die zij graag in het onderzoek zien terugkomen. Deze zijn hierna opgenomen. Voor deze aandachtsgebieden zijn geen normen vastgesteld. Wel zijn de doelen van de aandachtsgebieden opgenomen.

5.1. Gebruik Big data en data-analyse

Doel

De gemeente wil Big data en data-analyse inzetten. Geschiedt de inrichting hiervan conform wet- en regelgeving? Gebeurt dit ook veilig en hoe kwetsbaar is dat?

Deelvragen

1. Voldoet de gemeente Etten-Leur aan wet- en regelgeving aangaande de inzet van big data en data-analyse?
2. Is de ambtelijke organisatie voldoende toegerust (qua kennis en kunde) om, op een veilige manier en conform wet- en regelgeving, big data en data-analyse in te zetten?
3. Op welke wijze kan de gemeenteraad hier nog extra richting meegeven? Is er een handelingsperspectief te bedenken voor de gemeenteraad?

Bevindingen

In de organisatie wordt gebruik gemaakt van Big Data en data-analyse. In het privacybeleid en -reglement is vastgelegd dat de gemeente Etten-Leur gebruik kan maken van Big Data wanneer hierbij geanonimiseerde data worden gebruikt en alleen verzameld worden voor het betreffende onderzoek.

Dashboards kunnen aangevraagd worden bij de data-analisten door afdelingen, hiervoor vullen zij een onlangs ontwikkeld intakeformulier in. De dashboards die gebruikt worden door afdelingen worden door de data-analisten gemaakt. Deze data-analisten zitten in team Informatie, net als de Security Officer en de Privacy Officer. Het team bestaat uit 25 medewerkers en er zijn korte lijnen naar informatiebeveiliging en privacy. Wanneer daar aanleiding toe is worden verzoeken besproken met de Security Officer, Privacy Officer en/of Functionaris Gegevensbescherming en wordt de impact bepaald op informatiebeveiliging en privacy. Dit is niet in een formeel proces verankerd. Onderzoekers hebben geen verslagen van deze beoordelingen geconstateerd. Geïnterviewden geven aan dat gegevens geanonimiseerd worden ingevoerd.

Vorig jaar, 2018, is een week van de data-analyse georganiseerd in de organisatie door team Informatie. Tevens wordt het zogenaamde dataspel gebruikt om aan de bewustwording bij medewerkers te werken over zaken die wel en niet kunnen/mogen met data-analyse. Dashboards worden niet aangepast door de afdelingen zelf, altijd door team Informatie. Wanneer bronnen aan elkaar worden gekoppeld gaat dit altijd via data-analisten de Security Officer en de Privacy Officer, waar nodig, betrekken.

Tijdens het gesprek met een aantal raadsleden is dit thema ook besproken. Zie aldaar '5.3 Kaderstellende en controlerende rol gemeenteraad' voor de bevindingen.

Beantwoording deelvragen

1. Voldoet de gemeente Etten-Leur aan wet- en regelgeving aangaande de inzet van big data en data-analyse?
Er is nog geen heel duidelijke wet- en regelgeving rondom het gebruik en de inzet van big data en data-analyse. De gemeente heeft in het privacybeleid- en reglement vastgelegd dat gebruik gemaakt kan worden van big data en data-analyse zolang gebruik gemaakt wordt van geanonimiseerde gegevens. Dit is in lijn met wat de Algemene Verordening Gegevensbescherming (AVG) hierover zegt.

2. Is de ambtelijke organisatie voldoende toegerust (qua kennis en kunde) om, op een veilige manier en conform wet- en regelgeving, big data en data-analyse in te zetten?
Dashboards kunnen niet aangepast worden door afdelingen zelf. Alleen een selecte groep medewerkers van data-analisten die kennis en ervaring heeft met het maken van dashboards, bij het team Informatie, hebben die mogelijkheid. Wanneer bepaalde bronnen aan elkaar gekoppeld worden consulteren data-analisten de Privacy Officer en de Security Officer. Deze hebben voldoende kennis om conform wet- en regelgeving op het gebied van privacy en informatieveiligheid te adviseren over big data en data-analyse.

3. Op welke wijze kan de gemeenteraad hier nog extra richting meegeven? Is er een handelingsperspectief te bedenken voor de gemeenteraad?
Als gezegd zijn er nog weinig landelijke kaders, waardoor de gemeente, net als veel gemeenten, aangewezen is op haar eigen kennis, ervaring en interpretatie bij het toepassen van big data en data-analyse. Het zou goed zijn als de gemeenteraad de ambtelijke organisatie daarin helpt door eigen kaders te formuleren met betrekking tot het gebruik van big data en data-analyse, daarbij gebruik maken van de reeds aanwezige kennis en expertise van de ambtelijke organisatie.

Conclusies

Allereerst moet vastgesteld worden dat big data en data-analyse, landelijk gezien, nog in de kinderschoenen staat. Dit zorgt ervoor dat er nog geen hele duidelijke kaders zijn wat wel en niet is toegestaan. De gemeente Etten-Leur heeft zelf een aanzet gedaan tot het opstellen van zulke kaders door big data en data-analyse op te nemen in het privacybeleid en -reglement. Dit geeft de organisatie enige kaders bij het gebruik ervan. Zo wordt gebruik gemaakt van geanonimiseerde gegevens wat in lijn is met de Algemene Verordening Gegevensbescherming (AVG). Het ontwikkelen en beheren van dashboards is belegd bij het team Informatie, waar de kennis en expertise aanwezig is hiervoor, maar waar ook de kennis en expertise aanwezig is op de onderwerpen informatieveiligheid en privacy. Hiermee houdt de organisatie grip op het verder ontwikkelen en toepassen van big data en data-analyse. Naast deze centralisatie van ontwikkeling en gespecialiseerde kennis rondom big data en data-analyse wordt ook kennis en bewustzijn gecreëerd over deze onderwerpen bij de afdelingen. Door het spelen van een dataspel komen medewerkers in aanraking met big data en data-analyse en worden ze bewust gemaakt van de (on)mogelijkheden hiervan.

Geconcludeerd wordt dat de gemeente Etten-Leur een eigentijdse aanpak heeft voor het toepassen van big data en data-analyse. Hierbij wordt rekening gehouden met de, summiere, kaders die gegeven worden op deze onderwerpen en heeft de organisatie zelf kaders beschreven.

Risico's

Door het ontbreken van duidelijke landelijke kaders en wet- en regelgeving is het soms moeilijk om te bepalen hoever big data en data-analyse doorgevoerd en gebruikt kan worden. Het risico is dat er te ver gegaan wordt met experimenteren, waardoor er datalekken ontstaan of waardoor beslissingen genomen worden op basis van verkeerde of onvolledige informatie.

Aanbevelingen

Bij inzet van big data en data-analyse is het van belang dat er kleine stappen gezet worden. Zorg ervoor dat kennis en ervaring opgedaan wordt middels pilots die onderwerpen betreffen die niet direct een enorme invloed hebben op de Etten-Leurse samenleving. Hierdoor kan de organisatie leren en kennis en expertise ontwikkelen. Van belang hierbij is dat elke pilot goed geëvalueerd wordt met betrokkenen uit verschillende organisatieonderdelen (zo ook informatieveiligheid en privacy) en dat, waar nodig, de kaders voor de inzet en het gebruik van big data en data-analyse doorontwikkeld worden. Omdat er nog weinig landelijke kaders zijn, is het raadzaam dat de gemeenteraad kaders stelt op dit nieuwe onderwerp. Aanbevolen wordt om gebruik te maken van de reeds aanwezige kennis en expertise binnen de ambtelijke organisatie.
Sluit daarbij zoveel mogelijk bij regionale en landelijke ontwikkelingen, zoals bijeenkomsten en congressen van VNG (Realisatie).

5.2. Dataminimalisatie, eenmalige gegevensverstrekking en samenbrengen persoonsgegevens in klantprocessen (met name Sociaal Domein)

Doel

Hoe wordt een balans gevonden tussen 'alles willen weten' en het borgen van proportionaliteit en dataminimalisatie in klantprocessen? Hoe wordt daarbij voorkomen dat de inwoner steeds dezelfde gegevens moet afgeven bij verschillende afdelingen?

Deelvragen

1. Hoe wordt in de digitale dienstverlening de afweging gemaakt tussen dataminimalisatie en het streven naar eenmalige gegevensuitvraag?
2. Hoe is in het sociaal domein geborgd dat in beleids- en uitvoeringsprocessen het gebruik en samenbrengen van persoonsgegevens verloopt volgens de landelijke en gemeentelijke richtlijnen?

Bevindingen

Er is een gemeentebreed privacybeleid en -reglement aanwezig. Hier is dataminimalisatie onderdeel van. Het hergebruiken van gegevens is onderdeel van dit beleid. Hierin is opgenomen dat dit getoetst wordt aan de mogelijke inbreuk op de persoonlijke levenssfeer en wordt de afweging gemaakt om dit wel of niet te hergebruiken.

Binnen het Sociaal Domein zijn zowel een Privacybeleid, specifiek voor het Sociaal Domein, als Privacyprotocollen voor gegevensverwerking voor Jeugdhulp en Maatschappelijke Ondersteuning vastgesteld. Hierin staat onder andere beschreven welke informatie wel en niet wordt vastgelegd. Ook is hierin vastgelegd wanneer gegevensdeling binnen de verschillende domeinen wel en niet is toegestaan. Dit beleid en deze protocollen zijn gebaseerd op de Algemene Verordening Gegevensbescherming (AVG), domeinspecifieke wet- en regelgeving en landelijke standaarden.

Beantwoording deelvragen

1. Hoe wordt in de digitale dienstverlening de afweging gemaakt tussen dataminimalisatie en het streven naar eenmalige gegevensuitvraag?
In het gemeentebrede privacybeleid en –regelement is opgenomen dat dataminimalisatie wordt toegepast. Bij het hergebruik van gegevens (wat onderdeel is van hetzelfde beleid) wordt dit hergebruik getoetst aan de mogelijke inbreuk op de persoonlijke levenssfeer. Op deze wijze wordt de afweging gemaakt tussen dataminimalisatie en het streven naar eenmalige gegevensuitvraag.

2. Hoe is in het sociaal domein geborgd dat in beleids- en uitvoeringsprocessen het gebruik en samenbrengen van persoonsgegevens verloopt volgens de landelijke en gemeentelijke richtlijnen?
Het Sociaal Domein heeft een specifiek Privacybeleid alsook specifieke Privacyprotocollen voor gegevensverwerking bij Jeugdhulp en Maatschappelijke Ondersteuning. Hierin is beschreven welke informatie wel en niet wordt vastgelegd en welke gegevensdeling wel en niet zijn toegestaan. Dit beleid en deze protocollen zijn gebaseerd op wet- en regelgeving als de AVG en domeinspecifieke wet- en regelgeving.

Conclusies

Conclusie is dat dataminimalisatie en hergebruik van gegevens onderdeel zijn van het gemeentebrede privacybeleid en –reglement. In het specifieke Privacybeleid en de privacyprotocollen voor het Sociaal Domein is specifieker beschreven welke informatie wordt vastgelegd en gedeeld. Dit alles is op basis van de voorschriften uit de Algemene Verordening Gegevensbescherming (AVG) en domeinspecifieke wet- en regelgeving. Daarmee wordt geconcludeerd dat er duidelijke kaders zijn voor vastlegging van gegevens en het delen van gegevens, waarmee de organisatie in staat gesteld wordt zelf een afweging te maken.

Risico’s

Risico’s bij eenmalige vastlegging, meervoudig gebruik is dat er gegevens gedeeld worden tussen organisatieonderdelen dat niet is toegestaan. Door middel van kaders probeert de gemeente de medewerkers handvatten te bieden om de afweging te maken wanneer wel en niet te delen en welke informatie wel en niet op te vragen en daarmee de risico’s in te perken.

Aanbevelingen

Het bieden van kaders door de gemeente is een goede stap om organisatieonderdelen zelf de juiste afwegingen te laten maken. Daarnaast is het belangrijk om de kennis en expertise over te dragen aan de afdelingen. Aanbevolen wordt om hierbij gebruik te maken

van de reeds lopen bewustwordingsactiviteiten en tevens opleidingen/trainingen te verzorgen voor medewerkers die hier in hun werkzaamheden mee te maken hebben, zoals binnen het Sociaal Domein.

5.3. Kaderstellende en controlerende rol gemeenteraad

Doel

De gemeenteraad stelt als kader dat informatie veilig moet worden verwerkt; hoe wordt de gemeenteraad geïnformeerd over het invullen van dit kader, moet zij niet frequenter worden geconsulteerd? En hoe kan zij zelf een actievere rol bij dit onderwerp innemen? Is dat ook gewenst?

Deelvraag

1. Hoe kan de gemeenteraad haar kaderstellende en controlerende rol invullen?

Bevindingen

Met het oog op de beantwoording van deze vraag is met een aantal raadsleden een gesprek gevoerd over de huidige en gewenste kaderstellende en controlerende rol. De bevindingen die horen bij deze onderzoeksvraag worden niet getoetst aan een norm omdat de beantwoording ervan meer past bij een aanbeveling in plaats van een beoordeling of conclusie.

In een gesprek met een aantal raadsleden is door hen aangegeven dat informatiebeveiliging en privacy als een belangrijk onderwerp wordt gezien maar dat zij instrumenten zoeken om op deze thema's te kunnen sturen en de uitvoering van beleid te kunnen controleren. Binnen de P&C-cyclus wordt aan het onderwerp aandacht besteed, maar de gemeenteraad vraagt zich af of dit voldoende is.

Vanuit de ambtelijke organisatie zijn raadsleden uitgenodigd om deel te nemen aan het bewustwordingsspel dat voor de ambtenaren was ontwikkeld. Deelname was vrijblijvend. In totaal hebben 2 raads- of burgerleden deelgenomen.

Raadsleden geven desgevraagd aan dat zij in toenemende mate het belang zien van het bespreken van ethische aspecten en dilemma's rond het gebruik van data en van persoonsgegevens in het bijzonder. Op dit thema zien zij mogelijkheden om scherper kaders te stellen bij bijvoorbeeld big-datatoepassingen. Tegelijkertijd is het volgens de raadsleden wel nodig om meer samenhangende kennis te verkrijgen voordat het gesprek over meer inhoudelijke kaders kan worden gevoerd.

Beantwoording deelvragen

1. Hoe kan de gemeenteraad haar kaderstellende en controlerende rol invullen?

De gemeenteraad kan haar kaderstellende en controlerende rol versterken door haar interesse in de onderwerpen informatieveiligheid en privacy om te zetten in een meer actieve houding. Dit kan door meer zelf het gesprek over deze onderwerpen te entameren bij collegevoorstellen. De gemeenteraad draagt daarmee bij aan de meer planmatige aanpak die in de ambtelijke organisatie noodzakelijk is. Hiervoor is wel meer kennis en inzicht nodig in de onderwerpen 'informatieveiligheid' en 'privacy'.

Conclusies

De onderwerpen 'informatieveiligheid' en 'privacy' zijn in toenemende mate van belang uit oogpunt van continuïteit van de dienstverlening, de beveiliging van persoonsgegevens, de financiële middelen die er mee gemoeid zijn en de mate waarin voldaan wordt aan wet- en regelgeving. Een aantal raadsleden tonen actieve interesse in de onderwerpen. Dit betekent ook dat voor een groot deel van de gemeenteraad dat niet het geval is. Informatieveiligheid en privacy moeten als thema nog hun plek veroveren in de prioriteitsstelling van de gemeenteraad.

Risico's

Op de korte termijn zijn er geen bijzondere risico's. Wel is het zo de gemeenteraad nu al de kansen mist om zich beter te laten informeren over hoe de gemeente om gaat met informatieveiligheid en privacy en geen invloed uitoefent op ethische vraagstukken die rond het gebruik van persoonsgegevens (kunnen gaan) spelen. Daarnaast ontbreekt het raadsleden aan voldoende beoordelingskader om investeringen en initiatieven in informatieveiligheid en privacy te beoordelen en te controleren.

Aanbevelingen

De gemeenteraad kan door te investeren in kennis en inzicht, het ontwikkelen van handelingsrepertoire en door een meer actieve houding meer bereiken vanuit de kaderstellende en controlerende rol. Gezien het in de ambtelijke organisatie aanwezige kennisniveau en de bereidheid en het vermogen om dit over te brengen, kan dit prima samen met de ambtelijke organisatie vorm worden gegeven.

5.4. Casus: Automatisering gemeenteraad

Doel

Veilige omgang van de automatisering (tabletomgeving, applicaties en e-mail) door de gemeenteraad

Deelvraag

1. Hoe is de automatisering (de tablet-omgeving) van de Raad ingepast in gemeentelijke databeveiliging en hoe worden raadsleden hierover door de ambtelijke organisatie geïnformeerd? Het gaat hierbij zowel over hard controls (techniek) als soft controls (houding & gedrag)

Bevindingen

Uitgifte

Burger- en gemeenteraadsleden hebben een iPad ontvangen van de griffie. Hiervoor ondertekenen burger- en gemeenteraadsleden een zogenaamde bruikleenovereenkomst. Door ondertekening van deze bruikleenovereenkomst verplicht de gebruiker zich tot het zorgvuldig ("als een goed huisvader") omgaan met de iPad.
Voor de inkoop van de iPads zijn meerdere offertes opgevraagd, waaronder bij ICT West-Brabant West (ICT WBW) en consumentenwinkels. Uiteindelijk is omwille van prijs gekozen voor het aankopen van de iPads bij een consumentenwinkel. Hierbij is rekening gehouden

met het Inkoopbeleid en het 'Bring Your Own Device'-beleid van de gemeente Etten-Leur. De apparaten zijn op een gezamenlijke avond namens de griffie uitgereikt en raads- en burgerleden hebben daarbij een korte uitleg (knoppencursus) over de werking van het apparaat gehad. De apparaten kwamen nieuw uit de doos en er was dus niets voorgeïnstalleerd.

Gebruik
De gebruiker is, door ondertekening van de bruikleenovereenkomst, gehouden aan gedragsregels voor gebruik. Tijdens het gebruik wordt de iPad niet door de gemeente, of door ICT WBW voorzien van software en/of (beveiligings)updates. Dit is de verantwoordelijkheid van de raads- en burgerleden zelf. Ook het aan-/uitzetten van een toegangscode is verantwoordelijkheid van de gebruiker en wordt niet afgedwongen door software. De standaard toegangscode bij iPads is '0000'.

De iPad wordt uitgegeven voor het gebruik van het raadsinformatiesysteem 'iBabs'. De raads- en burgerleden zijn zelf verantwoordelijk voor het installeren van deze software. Er wordt een account aangemaakt voor burger- of raadslid door de griffie. Dit account wordt aangemaakt middels de privé e-mailadressen van de gebruikers, aangezien zij niet in het bezit zijn van een gemeentelijk e-mailadres. Het presidium heeft eerder aangegeven de kosten voor een gemeentelijk e-mailadres te hoog te vinden.

Het gebruik van 'iBabs' is mogelijk op twee manieren. Allereerst is deze benaderbaar via een zogenaamde webapp. Dit betekent dat 'iBabs' benaderd kan worden via een browser, zoals 'Safari' (standaard bij iPads), 'Chrome' of 'Internet Explorer'. Dit houdt in dat 'iBabs' via elk willekeurig apparaat te benaderen is, dus ook via privé apparatuur. Wanneer je inlogt via de webapp moet je inloggen met de verstrekte inloggegevens (gebruikersnaam en wachtwoord). Bij het inloggen is het mogelijk te kiezen voor de optie 'wachtwoord onthouden', waardoor daarna niet nogmaals om het wachtwoord gevraagd wordt, maar direct wordt ingelogd wanneer naar de webapp (via de browser) wordt gegaan. De geïnterviewde raadsleden geven aan dat wanneer gebruik gemaakt wordt van de webapplicatie, via de uitgegeven iPad, op kantoor of via privé-apparaten, geopende raadsstukken automatisch worden gedownload op het apparaat, zodat deze op het apparaat geopend kunnen worden.

Naast de webapplicatie is het mogelijk om de applicatie te installeren vanuit de Apple Store. Wanneer de applicatie van 'iBabs' wordt gebruikt dan worden de documenten die klaar staan bij inloggen, automatisch op het apparaat gedownload, zodat deze offline in te zien zijn. Inloggen in de applicatie vindt plaats via een wachtwoord. Het is mogelijk dit wachtwoord op te slaan, waardoor deze niet telkens opnieuw ingevoerd hoeft te worden. Raadsleden geven aan dat het mogelijk is om de vingerafdrukscanner te gebruiken als inlogmethode, maar dit is aan de gebruiker zelf en geen verplichting.

Inleveren
De griffie geeft aan dat de iPads na aftreden worden ingeleverd en daarna worden geschoond door ICT WBW. Enkele raadsleden geven aan dat in het verleden de keuze werd geboden om aan het einde van de raadsperiode de iPad in te leveren of tegen betaling over te nemen. Bij overname vond geen controle plaats of de gegevens op de iPad waren verwijderd. Vanaf deze raadsperiode is overname van de iPad op basis van het nieuwe rechtspositiebesluit niet langer mogelijk.

Beantwoording deelvragen

1. Hoe is de automatisering (de tablet-omgeving) van de Raad ingepast in gemeentelijke databeveiliging en hoe worden raadsleden hierover door de ambtelijke organisatie geïnformeerd? Het gaat hierbij zowel over hard controls (techniek) als soft controls (houding & gedrag)

De tablet-omgeving van de Raad staat los van de gemeentelijke databeveiliging. Dit komt omdat de tablets niet via ICT WBW of de gemeentelijke organisatie zijn ingekocht, maar zelf zijn aangeschaft door de griffie. De tablets worden niet voorzien van beveiligingsinstellingen, -updates en software door de gemeentelijke organisatie. De gebruiker is hiervoor zelf verantwoordelijk.
Hierdoor is het niet aan de ambtelijke organisatie om de burger- en raadsleden te informeren hierover. Dit gebeurt dan ook niet, los van de reeds lopende bewustwordingsactiviteiten welke tevens toegankelijk zijn voor burger- en raadsleden.
Er wordt door de gebruikers wel een bruikleenovereenkomst ondertekend, waarin de gebruikers worden verwezen naar het beleid van de gemeente.

Conclusies

De conclusie is dat de automatisering van de gemeenteraad niet voldoet aan het door de gemeente gestelde niveau van beveiliging. De tabletomgeving wordt niet beheerd door de gemeente, maar is de verantwoordelijkheid van de gebruiker zelf. Hierdoor is er onvoldoende beheer op de installatie van beveiligingsinstellingen, -updates en software. Daarnaast worden privé e-mailadressen gebruikt door burger- en raadsleden voor communicatie onderling en met inwoners.

Risico's

Gebruikers van automatisering hebben niet de kennis en expertise om deze automatisering op een goede manier te beveiligen. Doordat de verantwoordelijkheid voor het beveiligen van apparaten nu bij burger- en raadsleden ligt, ontstaat er een groot risico dat niet alle apparaten even goed beveiligd zijn. Dit risico kan uitmonden in het openbaar worden van informatie en gegevens die dat niet hadden mogen zijn. Dit brengt weer mogelijke datalekken met zich mee.
Het gebruik van privé e-mailadressen is een groot risico, omdat niet duidelijk is waar de mail wordt opgeslagen, waardoor het gebruik mogelijk in strijd is met de Algemene Verordening Gegevensbescherming (AVG). Daarnaast zijn privé mailadressen zeer kwetsbaar voor hackers, waarvan we de afgelopen jaren meerdere voorbeelden hebben gezien bij bijvoorbeeld minister Kamp[15] en Hilary Clinton[16].

Aanbevelingen

Zorg ervoor dat burger- en raadsleden op zeer korte termijn over e-mailadressen beschikken van de gemeentelijke organisatie. Daarbij dient grote aandacht te zijn voor het feit dat burger- en raadsleden voor hun werk als burger- of raadslid alleen nog maar via dat mailadres communiceren.
Daarnaast is het advies om de tabletomgeving van burger- en raadsleden onder te brengen in de gemeentelijke omgeving en het (beveiligings)beheer uit te laten voeren door ICT WBW.

[15] https://www.nrc.nl/nieuws/2016/05/12/minister-kamp-kreeg-werkmail-op-gmailaccount-a1407311
[16] https://nos.nl/artikel/2115588-fbi-onvoorzichtige-clinton-niet-vervolgen-om-privemails.html

In deze veranderingen kan dan direct door de ambtelijke organisatie zorggedragen worden voor voldoende kennisoverdracht op het gebied van gebruik, beveiliging en uiteraard privacy.

6. Conclusies, aanbevelingen en beantwoording centrale onderzoeksvraag

In dit rapport is verslag gedaan van het onderzoek van de rekenkamer naar databeveiliging binnen de gemeente Etten-Leur. In dit hoofdstuk worden op basis van de verkregen informatie en de reeds getrokken deelconclusies in de verschillende paragrafen, algehele conclusies getrokken. In de verschillende paragrafen zijn op de deelgebieden reeds aanbevelingen gedaan. In dit hoofdstuk worden de belangrijkste aanbevelingen nogmaals uiteengezet. Daarnaast wordt de centrale onderzoeksvraag beantwoord.

6.1. Conclusies

Algemeen wordt geconcludeerd dat de gemeente Etten-Leur databeveiliging serieus aanpakt. Er zijn functionarissen benoemd, er worden activiteiten ontplooid voor het verhogen van de bewustwording binnen de organisatie en er zijn op operationeel niveau meerdere acties opgepakt om het niveau van informatieveiligheid en privacy te verhogen binnen de organisatie. De onderzoekers zijn dan ook van mening dat er veel en goed werk wordt verzet door vele medewerkers binnen de organisatie op dit vlak.

Daarbij wordt geconcludeerd dat vele activiteiten op een informele manier worden opgepakt. Een volledige Plan Do Check Act cyclus (zie paragraaf 2.6), waarbij op een planmatige wijze[17], op basis van risico's en toetsing, door bestuur en management wordt bepaald welke activiteiten jaarlijks worden opgepakt, ontbreekt. Hierdoor ontstaat het risico dat bestuurders niet voldoende informatie hebben om goed te (be)sturen. Dit maakt het voor de ambtelijke organisatie moeilijker om de juiste koers aan te houden. Doordat de 'check' nog niet is ingericht, is onvoldoende inzichtelijk of maatregelen het effect bereiken wat van tevoren beoogd wordt. Daarnaast kunnen deze inzichten een basis vormen om bij te sturen in de act-fase.

Daarbij wordt nog niet planmatig getoetst op de naleving van het beleid door de lijnorganisatie. Informatieveiligheid en privacy zijn geen onderdeel van een intern controleplan, waar de naleving van het informatieveiligheidsbeleid en het privacybeleid, door afdelingen, in wordt getoetst.

6.2. Aanbevelingen

Aanbevolen wordt om informatieveiligheid en privacy op een planmatige manier te borgen in de organisatie. Er is reeds beleid geformuleerd waar op voortgeborduurd kan worden. Bepaal periodiek (bijvoorbeeld jaarlijks) op basis van risico's welke activiteiten in die periode ontplooid worden. Wijs verantwoordelijken aan en stuur op en rapporteer over de voortgang aan bestuur en management. Daarbij is het van belang dat er voldoende capaciteit en middelen beschikbaar gesteld worden die recht doen aan het ambitieniveau.

Daarmee wordt direct aanbevolen om de huidige beschikbare capaciteit en middelen nog eens goed door te lichten. In vergelijking met gemeenten van soortgelijke omvang zit de

[17] waar wil de organisatie aan voldoen en wat het in een bepaalde periode wordt opgepakt (Plan); het daadwerkelijk uitvoeren van deze planning door het toewijzen van verantwoordelijken en het periodiek rapporteren over de voortgang (Do); het toetsen van de effectiviteit van geïmplementeerde maatregelen (Check); en het waar nodig bijstellen van de maatregelen en planning (Act),

gemeente Etten-Leur aan de onderkant van de beschikbare capaciteit voor de rollen/functies van Privacy Officer, Security Officer en Functionaris Gegevensbescherming. Neem de functies van Security Officer en Privacy Officer, inclusief taken, verantwoordelijkheden en formatie, op in het functieboek. Houd daarbij rekening met het gegeven dat het coördinerende en adviserende functies zijn en dat de informatieveiligheid en privacy te allen tijde een lijnverantwoordelijkheid zijn. In totaal heeft de gemeente Etten-Leur hier 1 – 1,5 FTE voor beschikbaar (zie paragraaf 2.2), terwijl gemiddeld bij soortgelijke gemeenten 1,5 -2 FTE gebruikelijk is (zie paragraaf 1.4). Daarnaast moet voor het implementeren van maatregelen binnen de afdelingen steeds opnieuw budget aangevraagd worden. Het advies is om een voldoende structureel budget in de begroting op te nemen voor het implementeren van maatregelen voor informatieveiligheid en/of privacy.

6.3. Beantwoording onderzoeksvraag

Welk beleid heeft de gemeente Etten-Leur geformuleerd over databeveiliging en hoe wordt uitvoering aan dit beleid gegeven?

Etten-Leur heeft zowel een informatieveiligheidsbeleid, gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG), als een privacybeleid en –reglement, gebaseerd op de Algemene Verordening Gegevensbescherming (AVG) opgesteld en vastgesteld. Dit beleid vormt de basis voor databeveiliging binnen de organisatie.

Voor het uitvoering geven aan het beleid zijn rollen en verantwoordelijkheden toegekend aan verschillende medewerkers, zoals de Security Officer, de Privacy Officer en de Functionaris Gegevensbescherming (FG). Deze medewerkers werken aan bewustwording van de onderwerpen in de gehele organisatie door op een toegankelijke manier kennis en informatie over te brengen. Daarnaast zijn zij de adviserende organen op de onderwerpen binnen de organisatie en geven zij advies waar nodig.

Op dit moment is de uitvoering van het beleid nog erg informeel ingericht. Ondanks het goede werk dat verzet is, met name door de hierboven genoemde medewerkers, is het raadzaam om informatieveiligheid en privacy de aandacht te geven die het verdient en dat begint bij een formele verankering van de onderwerpen en de daarbij passende rapportagecyclus. Om te weten in hoeverre uitvoering wordt gegeven aan het beleid door de staande organisatie, moet dit onafhankelijk getoetst worden. Het wordt dan ook aanbevolen om informatieveiligheid en privacy een (grotere) rol uit te laten maken van het jaarlijkse controleplan. Met de inzichten kan sturing gegeven worden aan de uitvoering van het beleid door management en bestuur.

7. Reactie college op conceptrapport

Op 17 juli 2019 heeft de Rekenkamer het conceptrapport aangeboden voor bestuurlijk hoor en wederhoor. Het college heeft hierop gereageerd bij brief van 3 september 2019. De inhoud van deze brief is onderstaand integraal verwoord.

Geachte leden van de rekenkamer,

De Rekenkamer West-Brabant heeft in 2019 onderzoek verricht naar databeveiliging binnen de gemeente Etten-Leur. Dit onderzoek vinden wij belangrijk en nuttig. Wij willen de Rekenkamer hiervoor onze complimenten geven en bedanken voor de rapportage.

Op de onderzoeksbevindingen heeft de ambtelijke organisatie al eerder een reactie op uw opmerkingen gegeven; deze is voor het merendeel door uw Rekenkamer overgenomen. Bij deze geven wij u onze bestuurlijke reactie op de conclusies en aanbevelingen van het rapport.

Wij willen opmerken dat de interviews met medewerkers van de ambtelijke organisatie in maart 2019 gehouden zijn. Inmiddels heeft de gemeente verschillende verbeteringen doorgevoerd in het tijdbestek tussen het uitvoeren van het onderzoek en de periode voor bestuurlijk hoor- en wederhoor.

In onze reactie zullen wij omwille van de leesbaarheid de nummering aanhouden, zoals u deze ook in uw conceptrapportage heeft gehanteerd.

2.1. Beleid

Uw conclusie
U stelt dat het privacybeleid niet ter informatie naar de gemeenteraad is gegaan.

Onze reactie
In het rapport schrijft u op enkele plaatsen dat het privacybeleid en -reglement wel aan de gemeenteraad zijn verzonden. In uw conclusie geeft u aan dat dit niet het geval is.

Uw conclusie is niet juist. Het privacybeleid en -reglement zijn op 24 april 2018 ter kennisname aangeboden aan de gemeenteraad. Het specifieke beleid voor het Sociaal Domein is op 10 januari 2019 aangeboden.

2.2. Organisatie

Uw conclusie
In uw conclusies stelt u dat voor de rollen van Security Officer en Privacy Officer geen 0,5 – 1 FTE binnen hun functies aanwezig is.

Onze reactie
Wij delen deze conclusie niet. Beide functionarissen kunnen minimaal 70% van hun tijd besteden aan de invulling van hun respectievelijke rollen.

Uw aanbeveling
U beveelt aan dat zowel de Security Officer als de Privacy Officer volwaardige functies zouden moeten worden.

Onze reactie
Deze rollen zijn voldoende geborgd in de governance rondom dataveiligheid. Zoals hiervoor aangegeven hebben beide functionarissen voldoende tijd, middelen en de juiste verantwoordelijkheden om hun taak uit te kunnen voeren.

2.3. Personele beveiliging & Bewustwording

In algemene zin willen wij hier opmerken dat waar wordt gesproken over bewustwording op het onderwerp informatieveiligheid, tevens bewustwording op het gebied van privacy moet worden verstaan.

Uw conclusie
U concludeert dat deelname aan de bewustwordingsactiviteiten een vrijblijvend karakter heeft en niet verplicht is.

Onze reactie
Dit is niet helemaal juist. Deelname door iedereen wordt verwacht. Hier wordt over gerapporteerd aan het management, dat hier ook actief op stuurt. Er wordt daarbij uit gegaan van ieders eigen professionaliteit en verantwoordelijkheid.

Uw aanbevelingen
U beveelt aan om structureel budget te reserveren voor bewustwordingsactiviteiten, daarnaast beveelt u aan om het geautomatiseerde indienst- en uitdienstproces binnen een half jaar te evalueren en waar nodig bij te stellen.

Onze reactie
Al sinds enige jaren is er structureel budget aanwezig voor deze activiteiten. Goed dat u er op wijst het indienst- en uitdienstproces binnen een half jaar te evalueren. Deze aanbeveling nemen wij dan ook graag over.

2.5. Naleving

Uw conclusie
Er wordt vanuit Control op dit moment nog geen formele toetsing uitgevoerd op aspecten van informatieveiligheid en privacy. Hierdoor wordt de Plan-Do-Check-Act cyclus, zoals vastgelegd in het Informatiebeveiligingsbeleid, niet geheel doorlopen en vindt er, op deze wijze, geen onafhankelijke toetsing plaats op het naleven van procedures en de effectiviteit van beveiligingsmaatregelen en ingerichte processen.

Uw aanbevelingen
Stel jaarlijks een controleplan voor informatieveiligheid en privacy vast. Dit kan onderdeel zijn van een breder controleplan. Laat onder verantwoordelijkheid van Team Control controles uitvoeren, rapporteer hierover aan het management en doe daarbij voorstellen voor verbeteringen.

Onze reactie
De conclusie en aanbeveling rondom het inrichten van controlemechanismen om de werking van het informatieveiligheidsbeleid en het privacybeleid vast te stellen, onderschrijven wij.

Waar de Functionaris Gegevensbescherming haar focus in eerste instantie heeft gelegd op het creëren van voldoende basis, komen we nu in de fase dat we onder andere het cyclisch beheer meer aandacht moeten geven.

Hier zijn we ons van bewust en daar wordt aan gewerkt. Toetsing op de naleving van het informatieveiligheidsbeleid en privacybeleid zal dus zeker onderdeel vormen van het op te stellen interne controleplan.

3.1. Beheer van bedrijfsmiddelen

De organisatie is druk bezig met het maken van een overzicht van de voorzieningen. Veel, meest kritische, voorzieningen zijn in beeld, maar dit overzicht is nog niet actueel en volledig.

Wij verwachten in 2020 een volledig beeld te hebben.

3.3. Beheer van Communicatie- en bedienprocessen

Uw risico's
U geeft aan dat er een risico bestaat dat de gemeentelijke organisatie en ICT West-Brabant West (ICTWBW) langs elkaar heen werken, omdat de procedures voor wijzigingenbeheer niet op elkaar aansluiten.

Onze reactie
De gemeentelijke procedure wordt uitsluitend toegepast als het gaat om wijzigingen waarbij ICTWBW geen rol speelt. Denk hierbij aan software die op afstand bij een leverancier is geïnstalleerd, zogenaamde "Software as a service (Saas)".

Indien het een product betreft dat bij ICTWBW is geïnstalleerd, dan wordt gewerkt volgens de procedure van die organisatie.

ICTWBW bepaalt daarbij inderdaad de impact op systeemniveau. De betrokken Functioneel Beheerder van de gemeente bepaalt de impact op applicatieniveau. Deze test daarnaast de applicatie en adviseert de lijnmanager of de update in productie mag worden genomen.

Wanneer dat noodzakelijk is worden de Security Officer en/of Privacy Officer hierbij geconsulteerd.

Uw aanbeveling
U adviseert de wijzigingsprocessen van ICTWBW en van de gemeente zoveel mogelijk op elkaar af te stemmen.

Onze reactie
Gelet op het voorgaande heeft dit geen toegevoegde waarde, omdat het gemeentelijke proces uitsluitend wordt gevolgd in de situaties waarbij ICTWBW niet is betrokken.

3.5. Werking, ontwikkeling en onderhoud van informatiesystemen.

In algemene zin willen wij opmerken dat op diverse plekken in deze paragraaf wordt gesteld dat informatiebeveiliging en privacy geen vast onderdeel uitmaken van het inkoopproces.

Dit willen wij nuanceren. Er is wel een basis aanwezig. De organisatie moet, volgens het inkoopproces, de GIBIT-voorwaarden van toepassing verklaren als er sprake is van een ICT-component. Hierdoor zijn afdelingen verplicht afwegingen te maken die te maken hebben met privacy en informatieveiligheid.

De GIBIT-voorwaarden zijn op 26 september 2017 door ons college vastgesteld en sinds 1 november 2017 van kracht.

Uw aanbeveling
Aanbevolen wordt om informatieveiligheid en privacy vast onderdeel te laten zijn van inkoop- en aanbestedingstrajecten. Hiermee wordt aan de voorkant invulling gegeven aan systematieken als security- & privacy-by-design.

Onze reactie
Wij bedanken u voor deze aanbeveling en gaan bij de inkoop- en aanbestedingstrajecten meer aandacht geven aan informatieveiligheid en privacy. De GIBIT-voorwaarden vormen hiervoor een goede basis.

4.1. Rechten van betrokkenen

Uw aanbeveling
U stelt dat het proces zeer sporadisch wordt doorlopen en adviseert daarom het proces te evalueren iedere keer nadat het doorlopen is.

Onze reactie
Dit proces wordt weliswaar niet dagelijks, maar wel met enige regelmaat doorlopen. Het is daarom niet noodzakelijk het proces steeds nadat het doorlopen is te evalueren. Periodieke evaluatie volstaat. Omdat het een relatief nieuw proces betreft zal deze evaluatie vooralsnog wel frequenter plaatsvinden.

5.1. Gebruik Big data en data-analyse

Uw aanbeveling
Bij inzet van big data en data-analyse is het van belang dat er kleine stappen gezet worden. Zorg ervoor dat kennis en ervaring opgedaan worden middels pilots die onderwerpen betreffen die niet direct een enorme invloed hebben op de Etten-Leurse samenleving. Hierdoor kan de organisatie leren en kennis en expertise ontwikkelen. Van belang hierbij is dat elke pilot goed geëvalueerd wordt met betrokkenen uit verschillende organisatieonderdelen (zo ook informatieveiligheid en privacy) en dat, waar nodig, de

kaders voor de inzet en het gebruik van big data en data-analyse doorontwikkeld worden. Omdat er nog weinig landelijke kaders zijn, is het raadzaam dat de gemeenteraad kaders stelt op dit nieuwe onderwerp.

Aanbevolen wordt om gebruik te maken van de reeds aanwezige kennis en expertise binnen de ambtelijke organisatie. Sluit daarbij zoveel mogelijk aan bij regionale en landelijke ontwikkelingen, zoals bijeenkomsten en congressen van VNG (realisatie).

Onze reactie
Wij onderschrijven uw aanbeveling om met college en gemeenteraad te spreken over politiek filosofisch getinte vragen. Uitsluiting van deelname aan een gemeentelijke regeling mag bijvoorbeeld nooit een onbedoeld gevolg zijn van het datagedreven werken.

5.4. Casus: Automatisering gemeenteraad

Uw aanbevelingen
Zorg ervoor dat burger- en raadsleden op zeer korte termijn over e-mailadressen beschikken van de gemeentelijke organisatie. Daarbij dient grote aandacht te zijn voor het feit dat burger- en raadsleden voor hun werk als burger- of raadslid alleen nog maar via dat mailadres communiceren.
Daarnaast is het advies om de tabletomgeving van burger- en raadsleden onder te brengen in de gemeentelijke omgeving en het (beveiligings-)beheer uit te laten voeren door ICT WBW.
In deze veranderingen kan dan direct door de ambtelijke organisatie zorggedragen worden voor voldoende kennisoverdracht op het gebied van gebruik, beveiliging en uiteraard privacy.

Onze reactie
Het college vindt de automatisering van de gemeenteraad een groot risico. Wij adviseren de gemeenteraad heel nadrukkelijk om deze aanbevelingen over te nemen.

Met vriendelijke groet,
burgemeester en wethouders,

Dhr. drs. C. Smits	Mw. dr. M.W.M. de Vries
gemeentesecretaris	burgemeester

8. Nawoord

De Rekenkamer dankt het College voor haar bestuurlijke reactie waarin u aangeeft het onderzoek belangrijk en nuttig te vinden. Met de aanbevelingen kunt u ons inziens de borging van maatregelen rond informatieveiligheid verder versterken. Dat u al bent gestart met het implementeren van een aantal aanbevelingen wordt door ons dan ook als positief ervaren.
Hieronder gaan we op enkele onderdelen van uw reactie wat dieper in.

We zijn verheugd dat u aangeeft dat er voldoende tijd is voor de invulling van de functies van Privacy en Security Officer. U geeft aan dat betrokken medewerkers minimaal 70% van hun tijd kunnen besteden aan de invulling van hun rollen. Dit percentage sluit aan bij de inzet die wij passend achten in de ambtelijke organisatie van Etten-Leur.

U geeft aan dat in de rapportage wordt geconcludeerd dat het privacybeleid en - reglement niet naar de gemeenteraad is verzonden, terwijl in de bevindingen is opgenomen dat dit wel het geval is. Dit is inmiddels aangepast in de definitieve rapportage.

Bijlage 1: Gebruikte documentatie

Voorafgaand aan de interviews heeft documentstudie plaatsgevonden. Tijdens de interviews is extra documentatie opgevraagd. Hieronder vindt u een overzicht van de gebruikte documentatie en, wanneer van toepassing, de datum waarop het vastgesteld is en door wie het is vastgesteld.

Documentatie	**Vastgesteld door**	**Vastgesteld op**
Informatiebeleidsplan		
Informatieveiligheidsbeleid	College B&W	27 maart 2018
Informatiebeveiligingsplan		
Privacybeleid- en reglement	College B&W	24 april 2018
Privacybeleid Sociaal Domein	College B&W	8 januari 2019
Procedure melden beveiligingsincidenten	Informatiebeheerder	5 februari 2019
Rapportage beveiligingsincidenten	Security Officer	1 maart 2019
Procedure melden datalekken	Informatiebeheerder	5 februari 2019
Register van Verwerkingen		
Procedure in- en uitdienst		
Handleiding Checklist DPIA voor gemeenten		
PIA Rapportage Etten-Leur		
Prelightfull DPIA standaard		
Dienstverleningsovereenkomst ICTWBW	Loco-burgemeester	16 september 2015

Addendum DVO ICTWBW	Loco-burgemeester	23 mei 2017
Besluit GR ICTWBW	Burgemeester	23 mei 2017
PDC ICTWBW		
Maandelijkse rapportage SLR november 2018		
Service Level Agreement ICTWBW	Afdelingshoofd Concernondersteuning	8 oktober 2018
Procedure Rechten van Betrokkenen	Informatiebeheerder	5 februari 2019
Gegevensbescherming Jaarplan (Concept)		
Privacyprotocol Gegevensverwerking Jeugdhulp	College B&W	8 januari 2019
Privacyprotocol Gegevensverwerking maatschappelijke ondersteuning	College B&W	8 januari 2019
Procedure wijzigingsbeheer	Informatiebeheerder	28 februari 2019
Jaarrekening Etten-Leur 2017		
Verslag MT overleg d.d. 7 maart 2018		
MT Memo Samenwerken en werkruimte		
Bruikleenovereenkomst Mobile Devices Etten-Leur		
Adviesrapport IB ICTWBW		
Evaluatie Governance ICT WBW		
Baseline Informatiebeveiliging Gemeenten (BIG)		
Algemene Verordening Gegevensbescherming (AVG)		

10 Stappenplan Autoriteit Persoonsgegevens		
Informatieveiligheid Provincie Limburg - Zuidelijke Rekenkamer		
Onderzoek informatieveiligheid en privacy, gemeente Roosendaal		
Visie Control v1.0 (presentatie raad)		
Intake format (dashboard)		

Bijlage 2: Deelvragen en Normenkader

Onderdeel	Norm	Activiteiten
• Beveiligingsbeleid	• Er dient een informatieveiligheidsbeleid te zijn dat is goedgekeurd en uitgedragen door het hoogste management, vastgesteld door het college en bekendgemaakt bij de raad.	• Review van het informatieveiligheidsbeleid.
• Organisatie	• De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor informatieveiligheid worden toegekend en gecommuniceerd.	• Review van de beschrijving van de taken, bevoegdheden en verantwoordelijkheden. • Interview met de eindverantwoordelijke over de borging van de taken, bevoegdheden en verantwoordelijkheden.
• Beheer van bedrijfsmiddelen	• Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden. • Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met informatievoorzieningen.	• Beoordeling van de configuratie managementprocedure. • Interview met de systeembeheerder over de Configuratie Management Database (CMDB). • Analyse van de in gebruik zijnde devices en de wijze waarop deze zijn beveiligd.
• Personele beveiliging	• Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoort te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoort evenredig te zijn aan bedrijfseisen, classificatie van de informatie waartoe toegang wordt verleend en waargenomen risico's. • Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.	• Interview met P&O inzake het aannamebeleid. • Interview met P&O inzake de wijze waarop de betrokkenen bij de implementatie en controle op de informatieveiligheid worden gefaciliteerd in hun rol.
• Fysieke beveiliging	• Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te	• Fysieke inspectie van het gebouw. • Beoordeling van de procedure uitgifte tokens, sleutels, et cetera.

	beschermen waar zich informatie en ICT-voorzieningen bevinden.	
• Beheer van communicatie- en bedienprocessen	• Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben. • Bedieningsprocedures bevatten informatie over opstarten, afsluiten, back-up- en herstelacties, afhandelen van fouten, doorvoeren van wijzigingen, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging. • Er zijn procedures voor de behandeling van digitale media die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging.	• Interview met de systeembeheerder inzake de Information Technology Infrastructure Library (ITIL) procedures. • Review van de ITIL-procedures.
• Toegangsbeveiliging	• Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van organisatie-eisen en beveiligingseisen voor toegang.	• Beoordeling van het toegangsbeleid en de controle daarop.
• Verwerking, ontwikkeling en onderhoud van informatiesystemen	• In bedrijfseisen voor inkoop, gebouwaanpassingen, procesaanpassingen, nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.	• Interview met de inkoper over de wijze waarop bij inkoop rekening wordt gehouden met informatieveiligheid.
• Beheer van veiligheidsincidenten	• Informatieveiligheidsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd en op een adequate wijze te worden behandeld.	• Interview met de verantwoordelijken voor informatieveiligheid.
• Naleving	• Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.	• Inzage in controleactiviteiten en rapportage.

• ISMS	• Beoordeling van het Information Security Management System (ISMS).	• Beoordeling van de aanpak van de implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG). • Inzage in projectdefinitie, aanpak, samenstelling projectgroep en verslagen, inclusief de politieke verantwoording.

Onderdeel	Norm	Activiteiten
• Privacybeleid	• Er dient een privacybeleid te zijn dat is goedgekeurd en uitgedragen door het hoogste management, vastgesteld door het college en bekendgemaakt bij de raad.	• Review van het privacybeleid.
• Organisatie	• De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor privacy worden toegekend en gecommuniceerd.	• Review van de beschrijving van de taken, bevoegdheden en verantwoordelijkheden. • Interview met de eindverantwoordelijke over de borging van de taken, bevoegdheden en verantwoordelijkheden.
• Bewustwording	• Er dient periodiek aandacht te zijn voor bewustwording onder medewerkers op het gebied van privacy.	• Beoordeling van bewustwordingsactiviteiten als intranetberichten, bewustwordingssessies, notulen van afdelingsoverleggen.
• Rechten van betrokkenen	• Er behoort een proces ingericht te zijn waar inwoners hun rechten rondom hun persoonsgegevens kunnen uitoefenen.	• Interview met Functionaris Gegevensbescherming en/of Privacy Officer. • Beoordeling procedure rechten van betrokkenen. • Beoordeling vastgelegde reactie op ingekomen verzoeken.
• Register van verwerkingen	• Er behoort een actueel overzicht te zijn waar de organisatie persoonsgegevens verwerkt, inclusief (wettelijke) grondslag. • Ook dient een proces ingericht te zijn voor periodieke actualisatie van dit overzicht.	• Beoordeling aanwezige register van verwerkingen. • Beoordeling proces ter actualisatie.
• PIA	• Er is een proces ingericht voor het uitvoeren van Privacy Impact Assessments (PIA's).	• Beoordeling procedure uitvoeren PIA.

• Privacy-by-design	• Privacy behoort onderdeel te zijn van aanbestedingen (inclusief het afsluiten van verwerkersovereenkomsten) en projecten.	• Beoordeling inkoop- en aanbestedingsdocumenten. • Beoordeling projectplannen. • Beoordeling aanwezigheid verwerkersovereenkomsten. • Interview met inkoopfunctionaris.
• Meldplicht datalekken	• Er is een proces aanwezig en bekend bij medewerkers voor het melden van incidenten en de afhandeling van datalekken.	• Beoordeling procedure melden incidenten en afhandelen datalekken. • Interview met Privacy Officer en/of Functionaris Gegevensbescherming.
• Beheer van beveiligingsincidenten	• Informatieveiligheidsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd en op een adequate wijze te worden behandeld.	• Interview met de verantwoordelijken voor informatieveiligheid.
• Naleving	• Er is een controleplan waar privacy onderdeel van uitmaakt.	• Inzage in controleactiviteiten en rapportage.
• PMS	• Beoordeling van het Privacy Management System (PMS).	• Beoordeling van de aanpak van de implementatie van de Algemene Verordening Gegevensbescherming (AVG). • Inzage in projectdefinitie, aanpak, samenstelling projectgroep en verslagen, inclusief de politieke verantwoording.