Raadsinformatiebrief

Gemeente Albrandswaard

De gemeenteraad van Albrandswaard

Uw brief van:		Ons kenmerk:	211859
Uw kenmerk:		Contact:	H. de Groot
Bijlage(n):	1	Doorkiesnummer:	0180-451594
		E-mailadres:	h.groot@BAR-organisatie.nl
		Datum:	27 oktober 2020

Betreft: Rapport AVG Albrandswaard.

Geachte leden van de Raad,

INLEIDING

Het college van Albrandswaard laat jaarlijks verschillende onderzoeken uitvoeren naar de doelmatigheid en doeltreffendheid van beleid en uitvoering. Het afgelopen jaar is onderzoek gedaan naar de wijze waarop het uitvoeringsproces van de AVG is georganiseerd bij Albrandswaard. Met de uitvoering van dit onderzoek wordt mede invulling gegeven aan artikel 213a van de gemeentewet.

KERNBOODSCHAP

Onderzocht is welk beleid er is ten aanzien van de AVG in Albrandswaard, hoe dit beleid in de organisatie verankerd is en of er verbetermaatregelen nodig zijn.

CONSEQUENTIES

De aanbevelingen uit het rapport AVG nemen wij mee bij de al lopende verbeterprocessen binnen de organisatie.

VERVOLG

De directieraad van de BAR-organisatie heeft naar aanleiding van het rapport besloten om een programma Informatieveiligheid en Privacy op te starten die alle aanbevelingen uit het rapport zal meenemen in een verbetertraject. In een vervolgonderzoek door Concerncontrol zal worden nagegaan in hoeverre de verbeteracties zijn gerealiseerd en de aanbevelingen zijn opgevolgd. Dit vervolgonderzoek wordt uitgevoerd in 2021.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

BIJLAGEN

1. Het rapport AVG Albrandswaard (inclusief bijlagen)

Met vriendelijke groet,
het college van de gemeente Albrandswaard,
de secretaris, de burgemeester,

Hans Cats drs. Jolanda de Witte

`

Onderzoek

Algemene Verordening Gegevensbescherming (AVG)

Albrandswaard 2020

INHOUD

1 Aanleiding en doelstelling

1.1 Aanleiding van het onderzoek

In artikel 213a van de Gemeentewet is de eigen onderzoeksfunctie van het college geregeld. Dit artikel luidt:

“Het College verricht periodiek onderzoek naar de doelmatigheid en doeltreffendheid van het door het College gevoerde bestuur. De raad stelt bij verordening regels hierover.”

Albrandswaard geeft invulling aan de wet met het vaststellen van de Verordening (onderzoeken) doelmatigheid en doeltreffendheid. Deze verordening bepaalt dat het college jaarlijks preventief organisatiegericht onderzoek verricht bij een gemeentelijke afdeling en/of één themagericht onderzoek binnen de organisatie. Eén van de onderzoeken die Albrandswaard wenst uit te voeren is: “een onderzoek naar de uitwerking van de Algemene Verordening Gegevensbescherming (AVG) in de gemeente Albrandswaard.”

1.2 Algemeen

De Algemene verordening gegevensbescherming (AVG) is op 25 mei 2016 in werking getreden. Met ingang van 25 mei 2018 is de verplichting ingegaan dat decentrale overheden aan de regels uit de AVG moeten voldoen.

De regels omtrent gegevensbescherming waren voorheen geregeld in richtlijn 95/46/EG omtrent gegevensbescherming. Echter, tussen 1995 en nu is de samenleving gedigitaliseerd, is er een toename in dataverkeer en ontwikkelt de technologie zich steeds sneller. De wetgeving was dan ook toe aan vernieuwing. De EU is het na lange tijd eens geworden over de Algemene Verordening Gegevensbescherming **(**hierna: AVG), die in werking is getreden op 24 mei 2016 en op 25 mei 2018 van toepassing is geworden (art. 99 lid 2 AVG)**.**[1]

Doordat het wetgevingsinstrument een Europese verordening betreft, is deze verordening “verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat” (art. 99 lid 2 AVG).

1.3 Doelstelling van het onderzoek

Met dit onderzoek wil Albrandswaard een beeld krijgen van de stand van zaken van het huidige beleid, de uitvoering en de gevolgen hiervan voor de kosten ten aanzien van de AVG. Dit op basis van 10 onderzoeksvragen waarin verwijzingen zijn opgenomen naar het 10 stappenplan van de Autoriteit Persoonsgegevens.
De centrale vraagstelling van dit onderzoek is:

“In welke mate is uitvoering gegeven aan het 10-stappenplan van de Autoriteit Persoonsgegevens en is daarmee voldaan aan de “formele eisen” van de AVG”?

Met de conclusies en aanbevelingen uit het rapport willen we bereiken dat daar waar mogelijkheden zijn, verbeteringen worden gerealiseerd op het gebied van beleid, uitvoering en uitgaven ten aanzien van de AVG.

[1] Regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming)

1.4 Onderzoeksvragen

Er is een analyse uitgevoerd van het huidige beleid zoals dit is vastgesteld en de wijze waarop het beleid in de praktijk wordt uitgevoerd. We willen hierbij duidelijkheid krijgen in de volgende (proces)onderdelen:

Beleid

1. Welk beleid heeft de gemeente geformuleerd ter bescherming van persoonsgegevens in het kader van de Algemene Verordening Gegevensbescherming? (Betreft alle stappen van 10-stappenplan AP, zie bijlage 1.)

2. Op welke wijze komt het beleid tot uiting in de besluitvorming rondom gegevensverwerkingen en de financiering ervan? (Stappen 1, 4, 5 en 8 van 10-stappenplan AP.)

Uitvoering Beleid

3. In welke mate heeft de gemeente de verwerkingsactiviteiten die onder eigen verantwoordelijkheid of gezamenlijke verantwoordelijkheid vallen inzichtelijk gemaakt? (Stap 3 van 10-stappenplan AP.)

4. Op welke wijze heeft de gemeente het proces rondom het uitoefenen van rechten van betrokkenen, het geven van toestemming en het uitvoeren van DPIA's[2] in de organisatie ingebed? (Stappen 2, 4 en 10 van 10-stappenplan AP.)

Governance (intern en extern)

5. Hoe is uitvoering gegeven aan dit beleid of zijn rollen, verantwoordelijkheden en taken belegd in de organisatie ten aanzien van de gegevensbescherming? (Stap 6 van 10-Stappenplan AP.)

6. In hoeverre is de gemeente in control ten aanzien van de afspraken met derden rondom uitwisseling of verstrekking van persoonsgegevens? (Stap 8 van 10-stappenplan AP.)

Informatiebeveiliging

7. Welke stappen heeft de gemeente genomen om de bewustwording binnen de organisatie op niveau te houden? (Stap 1 van 10-stappenplan AP.)

8. Hoe zorgt de gemeente ervoor dat de beschikbaarheid, integriteit en de vertrouwelijkheid van de verwerking van persoonsgegevens gewaarborgd is en blijft? (Stappen 1 en 7 van 10-stappenplan AP.)

Verantwoording

9. Op welke wijze legt de gemeente verantwoording af ten aanzien van het borgen van de naleving van de AVG binnen de eigen organisatie, naar de betrokkenen, naar de Functionaris Gegevensbescherming en naar de AP toe?

10. Welke stappen moeten nog worden ondernomen om te voldoen en de AVG volledig binnen de gemeentelijke organisatie te implementeren zodat Albrandswaard voldoet aan de wettelijke eisen voor het verwerken en beveiligen van persoonsgegevens?

[2] Data Protection Impact Assessment/gegevensbeschermingseffectbeoordeling

1.5 Afkortingenlijst

AP Autoriteit Persoonsgegevens
AVG Algemene Verordening Gegevensbescherming (in het Engels: GDPR)
GDPR General Data Protection Regulation (in het Nederlands: AVG)
DPIA Data Protection Impact Assessment
FG Functionaris voor de gegevensbescherming
CISO Chief Information Security Officer
PO Privacy Officer

2 Werkwijze

2.1 Afbakening van het onderzoek

De onderzoeksvragen richten zich op: Beleid, Uitvoering van het Beleid, Governance (intern en extern), Informatiebeveiliging en verantwoording. Omtrent deze onderwerpen is informatie verzameld in dit onderzoek en zijn aanbevelingen gedaan om als gemeentelijke organisatie te voldoen aan de eisen van de AVG.
In dit onderzoek is in ieder geval niet meegenomen een analyse van de verwerkingen zelf en de vraag in hoeverre deze verwerkingen voldoen aan de vereisten van de AVG (materiele eisen AVG). In het onderhavige AVG-onderzoek staat met name de vraag centraal in hoeverre de minimale eisen zoals deze terugkomen in het 10-stappenplan van de AP zijn uitgevoerd.
Stap 5 uit het 10-stappenplan van de AP betreffende privacy by design en privacy by default zal buiten beschouwing blijven voor zover het gaat om de afzonderlijke verwerkingen. Uiteraard komt privacy by design en by default terug bij stap 4 (DPIA) en bij stap 1 (Bewustwording) voor zover het gaat om de organisatie brede vraagstukken. Stap 9 van het 10-stappenplan van de AP (Leidende toezichthouder) is voor de gemeente Albrandswaard niet aan de orde omdat stap 9 bedoeld is voor organisaties binnen een concern waarvoor één leidende toezichthouder wordt aangemerkt, en zal daarom niet worden getoetst. Tot slot wordt in dit onderzoek de toets of de gemeente Albrandswaard voldoet aan de eisen van de Baseline Informatiebeveiliging Overheid (BIO) buiten beschouwing gelaten en enkel genoemd als verwijzing. Informatiebeveiliging wordt enkel globaal meegenomen in dit onderzoek.

2.2 Onderzoeksaanpak

De Autoriteit Persoonsgegevens (AP) is de Nederlandse gegevensbeschermingsautoriteit en het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens. De organisatie houdt zich in dit kader bezig met privacy en gegevensbescherming.
De Functionaris Gegevensbescherming (FG) is de onafhankelijke interne) toezichthouder op de werking van de AVG in de BAR-organisatie en de drie gemeenten. In de AVG is geregeld dat de AP de FG als contactpersoon van de AP optreedt voor adviezen maar ook wanneer de gemeente Albrandswaard niet voldoet aan de eisen van de AVG[3].

Om dit onderzoek te realiseren is samenwerking gezocht met de FG die is aangesteld voor de gemeente Albrandswaard. Het toezichthouden op de naleving van de AVG in de gemeente Albrandswaard is een van de voornaamste taken van de FG. Het is daarom logisch dat dit onderzoek vanuit Concerncontrol in samenwerking met de FG geschiedt. De FG heeft inhoudelijke vragen geformuleerd waaraan de situatie bij de gemeente Albrandswaard zal worden getoetst. De vragen zijn gebaseerd op best practices zoals “Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie” van VNG Realisatie december 2018 en het “GDPR CARPA certification criteria” van CNPD oktober 2018. De geformuleerde vragen hebben geleid tot 10 onderzoeksvragen, waarin ook wordt verwezen naar het 10 stappenplan van de AP (zie Bijlage 1).
De FG zal uiteindelijk de resultaten van het onderzoek beoordelen en de organisatie van advies voorzien.

Vanuit Concerncontrol zijn vragen die de FG heeft opgesteld digitaal uitgezet bij 76 medewerkers van de BAR-organisatie. Nadat de medewerkers de vragen hebben beantwoord, is de output geanalyseerd.
Vervolgens zijn interview gesprekken uitgevoerd met 11 verschillende medewerkers, waarin:

- Dieper is ingegaan op ontbrekende AVG-maatregelen.
- Getracht is te achterhalen wat de precieze oorzaken van de praktische invoeringsproblemen zijn.
- Er is gezocht naar (haalbare) oplossingen die de risico’s bij het niet voldoen aan de AVG kunnen verminderen.

[3] Artikel 39 AVG: De FG is namens de organisatie de eerste contactpersoon voor de Autoriteit Persoonsgegevens.

Geïnterviewde medewerkers:

Functie	Cluster
Afdelingshoofd	Informatie & Automatisering
Afdelingshoofd	Juridische zaken & Inkoop
Inkoper	Juridische zaken & Inkoop
Contractbeheerder	Juridische zaken & inkoop
Controller	Maatschappij
Privacy Officer (tijdelijke inhuur)	Maatschappij
Applicatiebeheerder	Informatie & Automatisering
Stagiaire	Juridische zaken & Inkoop
CISO	Informatie & Automatisering
Privacy Officer	Juridische zaken & Inkoop
Functionaris Gegevensbescherming	Concerncontrol

Totaal heeft ruim 50% van de medewerkers op de digitale vragen gereageerd.

Er zijn in totaal 11 interviewgesprekken gevoerd. De enquêtevragen en de interviewgesprekken zijn organisatie breed ingestoken. Daarbij is gezocht naar zoveel mogelijk evenredige verdeling van functies die betrokken zijn in werkzaamheden waarin met persoonsgegevens wordt gewerkt. Ter verduidelijking wordt in de rapportage van dit onderzoek verwezen naar de opmerkingen die in de interview gesprekken zijn gedaan.

2.3 Wat zijn de risico's bij overtreding van de AVG?

Het doel van de AVG is "bescherming persoonsgegevens" van betrokkenen. Betrokkenen wil zeggen degenen over wie persoonsgegevens worden verwerkt en in het geval van gemeente Albrandswaard zijn dat de burgers en eigen ambtenaren. De AP houdt toezicht op degenen die op systematische wijze persoonsgegevens verwerken waaronder in ieder geval begrepen publieke organisaties en bedrijven. De AP kan bij het niet voldoen aan de eisen van de AVG-sanctiemaatregelen treffen. Met de inwerkingtreding van de AVG kunnen deze boetes oplopen tot maar liefst € 20 miljoen of 4% van de jaarlijkse globale omzet per overtreding. Voorbeelden van sancties zijn de opgelegde boete van 460.000 euro aan Haga Ziekenhuis aangevuld met een last onder dwangsom voor het niet op orde hebben van interne informatiebeveiliging /informatieveiligheid. Daarnaast hebben verzekeraars Menzins, VGZ en CZ ook lasten onder dwangsom gekregen voor het niet voldoen aan de AVG en zeer recent heeft de KNLTB (tennisbond) een bestuurlijke boete van 525.000 euro opgelegd gekregen voor het onrechtmatig delen van persoonsgegevens.

De sancties van de AP moeten echter niet de reden zijn om aan de AVG te voldoen. Het bovenstaande schetst enkel een beeld dat de AVG serieus moet worden genomen en niet alleen om boetes te voorkomen. Het gaat erom het vertrouwen van onze burger en medewerkers niet kwijt te raken en ook het voorkomen van negatieve pers, maar bovenal om zorgvuldig en verantwoord met hun gegevens om te gaan. Het niet volgens de AVG verwerken van persoonsgegevens kan een enorme impact op het privéleven van betrokkenen hebben en wij als gemeente hebben daarin een grote rol en verantwoordelijkheid. Betrokkenen hebben anderzijds ook rechten gekregen om controle op ons uit te oefenen maar ook het recht om een klacht in te dienen bij AP, schade te claimen via de rechter of bij de gemeente zelf. Ook zijn er inmiddels rechtszaken aangespannen door betrokkenen vanwege het niet voldoen aan de AVG. Tot slot, het verwerken van persoonsgegevens volgens de AVG zorgt ervoor dat wij iets meer in controle kunnen zijn over onze gegevenshuishouding, de genomen maatregelen en de te nemen acties bij datalekken, en om de continuïteit van onze bedrijfsprocessen beter kunnen waarborgen en wordt voldaan aan de compliance eisen uit de AVG.

3 Uitwerking onderzoeksvragen

3.1 Beleid

De volgende onderdelen zijn geformaliseerd:

- Informatiebeveiligingsbeleid (zie bijlage 2)
- Privacy beleid, Gemeente Albrandswaard 2019/2020 (zie bijlage 3)

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid systemen voor Gemeenten, Rijk, Waterschappen en Provincies.
Hiermee ontstaat één gezamenlijk normenkader voor informatieveiligheid binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. Het Privacy-beleid van de gemeente Albrandswaard is in werking getreden op 29 oktober 2019 en werkt met terugwerkende kracht vanaf 1 januari 2019.
De Chief Information Security Officer (CISO) zorgt op basis van de BIO-concern breed, voor beleid, coördinatie, advisering en rapportage over een samenhangend pakket aan maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening te waarborgen.
Het beleid is BIO proof gemaakt, omdat de BIG is vervallen. Daarnaast wordt er nog onderliggend beleid, zoals een cryptografiebeleid en logging beleid opgesteld dat wordt vastgesteld door de directie van de BAR-organisatie

De CISO (Chief Information Security Officer) rapporteert rechtstreeks aan het management (hoofd automatisering en informatie) van de BAR-organisatie. In zeer uitzonderlijke situaties zal de CISO rechtstreeks rapporteren aan de gemeentesecretaris.

Huidige resultaten van het beleid:

- Het Privacy beleid is vastgesteld
- Een verwerkingsregister is opgesteld en dit wordt bijgehouden
- Er zijn informatiebijeenkomsten georganiseerd waarin de FG informatie over de AVG heeft gegeven aan groepen medewerkers
- Verwerkingsovereenkomsten worden afgesloten
- DPIA (data protection impact assessments) worden steeds meer uitgevoerd
- Bewustwording wordt bevorderd door structureel informatie te geven over informatiebeveiliging en privacy, zoals onder andere op posters in de lift, scherminfo op de computer, berichten op BAR-plaza.
- Er is een procedure voor rechten betrokkenen die gevolgd wordt op het moment dat betrokkene een verzoek indient om zijn privacyrechten uit te oefenen.

De verantwoordelijkheid voor de informatiebeveiliging/privacybescherming (PIOFACH taken) en het implementeren van de informatiebeveiligingsmaatregelen ligt bij het (lijn)management (proceseigenaar). Binnen de ambtelijke organisatie is het lijnmanagement verantwoordelijk voor de integrale informatiebeveiliging van zijn of haar organisatieonderdeel, de bijbehorende informatiesystemen en gegevensverzamelingen. (Zie hiervoor pagina 5 in het informatiebeveiligingsbeleid van de gemeente).
Er zijn diverse beheertaken die uitgevoerd moeten worden om de structurele werkzaamheden die de gemeente Albrandswaard verricht of zou moeten verrichten om blijvend te voldoen aan de eisen die de AVG stelt. Bijvoorbeeld controles (conform art 32 lid 1 onder d AVG) op het gebied van informatieveiligheid (audits) en de naleving van de verwerkersovereenkomsten bij bewerkers, leveranciers en partners. Dit wordt nu niet uitgevoerd omdat hiervoor geen personele capaciteit beschikbaar is en er is ook geen procedure.

In de begroting van de BAR-organisatie is formatie voor de functies van FG, CISO en PO opgenomen.
Niet inzichtelijk is wat de kosten van de implementatie en naleving van de AVG voor de gemeente Albrandswaard zijn omdat de diverse activiteiten die betrekking hebben op AVG-maatregelen, zoals boven opgesomd, verspreid zijn over verschillende werkzaamheden van medewerkers binnen de BAR-organisatie waardoor niet inzichtelijk is wat daarvan de kosten zijn.

De werkzaamheden voor de AVG zijn niet eenmalig maar ze blijven een belangrijke voorwaarde om in de uitvoeringspraktijk van de werkzaamheden die de gemeente Albrandswaard verricht, blijvend te voldoen aan de eisen die de AVG stelt.
Deze werkzaamheden betreffen onder andere:

- DPIA's
- Verwerkingsovereenkomsten
- Verwerkingsregister
- Controles
- Audits
- Bewustwordingsmaatregelen
- E-learnings

1. **Periodieke controle van de autorisaties (toegangsrechten)** -> De verantwoordelijke manager (proceseigenaar) behoort de autorisaties (toegangsrechten) van gebruikers/beheerders tot de in het proces verwerkte gegevens en de gebruikte applicatie(s) regelmatig te beoordelen in een formeel proces (cyclisch proces). Hierbij dient te worden vastgesteld of de autorisaties (toegangsrechten) en veranderingen hierin juist en tijdig zijn aangebracht, de juiste functiescheiding is toegepast en wordt voldaan aan de principes van doelbinding en proportionaliteit en of er oneigenlijk autorisatie-toekenningen hebben plaatsgevonden.
2. **Periodieke controle van de logging** -> De verantwoordelijke manager (proceseigenaar) behoort de logging in te regelen en de log-informatie regelmatig monitoren (signaleren, analyseren rapporteren en bijsturen). Zodat tijdig correctieve maatregelen kunnen worden getroffen en om informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders om vast te stellen of onrechtmatige, onregelmatige of doel overschrijdende verwerking van gegevens heeft plaatsgevonden. Het resultaat van deze controleactiviteiten (analyseren rapporteren en bijsturen) behoort regelmatig (minimaal maandelijks) te worden beoordeeld en te gerapporteerd aan de verantwoordelijk manager (proceseigenaar). De taken op dit gebied dienen te zijn belegd en worden (structureel) uitgevoerd.
3. **Periodieke controle naleving van de verwerkersovereenkomsten bij bewerkers het gebied van informatieveiligheid (audits)** -> Controles uitvoeren conform art 32 lid 1 onder d AVG. Het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking en de naleving van de verwerkersovereenkomsten bij bewerkers, leveranciers en partners vinden niet plaats. Hiervoor is geen personele capaciteit beschikbaar en er is geen procedure.

De onderdelen 1 en 2 vallen onder de verantwoordelijkheid van de lijnmanager (proceseigenaar). De proceseigenaar (lijnmanagement) is onder andere verantwoordelijk voor de implementatie en het in stand houden van de informatieveiligheid en de bijbehorende informatiebeveiligingsmaatregelen binnen:

1. Het betrokken organisatieonderdeel en de processen;
2. De bijbehorende informatiesystemen (applicaties, procedures, enzovoorts), inclusief informatiesystemen die in de Cloud zijn ondergebracht;
3. De gegevensverzamelingen, inclusief gegevensverwerkingen (data) die in de Cloud zijn ondergebracht, of bij de ketenpartners.

Omdat de kosten niet inzichtelijk zijn wordt geadviseerd (ook door de FG) de AVG en de BIO structureel mee te nemen in de begroting van de BAR-organisatie en dit vervolgens te verrekenen naar de clusters. Daarnaast wordt aanbevolen dat de AVG in projecten moet worden geborgd. Dit houdt in dat een projectvoorstel in de begroting rekening moet houden met de AVG-toets.

3.2 Uitvoering Beleid

De BAR-organisatie heeft uitvoering gegeven aan het Privacy beleid door een verwerkingsregister op te stellen, een procedure rechten betrokkenen op te zetten en ernaar te handelen en bij voorgenomen verwerkingen een DPIA uit te voeren. Hieronder wordt per onderdeel toelichting gegeven.

Verwerkingsregister

De AVG heeft de verplichting (artikel 30) dat de organisatie over een verwerkingsregister beschikt waarin wordt bijgehouden welke persoonsgegevens worden verwerkt. Vastgelegd wordt onder andere op basis van welke wettelijke grondslag de gegevens worden verwerkt. Ook hoe de gegevens worden opgeslagen en hoe lang deze worden bewaard. De BAR-organisatie die voor de gemeente Albrandswaard gemeentelijke taken uitvoert, beschikt over een verwerkingsregister. Conform het bepaalde in het Privacy beleid is de wens van de PO dat het verwerkingsregister raadpleegbaar is op de gemeentelijke website. Het realiseren hiervan stuit op technische problemen waarvoor nog geen oplossing gevonden is. Hier wordt frictie geconstateerd in wat het Privacy beleid voorschrijft en wat niet wordt uitgevoerd, namelijk het verwerkingsregister raadpleegbaar op de gemeentelijke website.

Het verwerkingsregister wordt bijgehouden in de applicatie I-navigator. In deze applicatie zijn standaard de gemeentelijke processen opgenomen waarin met persoonsgegevens wordt gewerkt. Deze standaard van gemeentelijke processen is door de afdeling I-service zodanig bewerkt dat deze corresponderen met de werkwijze die de BAR-organisatie hanteert in haar werkprocessen. Totaal zijn er 1298 processen waarvan 724 processen die persoonsgegevens bevatten, in het verwerkingsregister zijn opgenomen.
De volgende bevindingen zijn gedaan wat betreft het register van verwerkingen:

- Er is geen procedure aanwezig waarin wijzigingen in processen wordt gemeld aan de beheerder van het verwerkingsregister.
- Hierdoor is het dan de vraag of de processen waarin verwerkingen van persoonsgegevens plaatsvinden compleet zijn in het register.
- Er vinden geen audits plaats op het verwerkingsregister.

De FG is van mening dat de gemeente Albrandswaard voor het huidige privacyvolwassenheidsniveau voldoet aan de eis om een register op te stellen. Het register voldoet echter niet als Albrandswaard een iets hoger privacyvolwassenheidsniveau bereikt. De FG is van mening dat de verwerkingen in hoofdlijnen zijn uitgewerkt waardoor het huidige register slechts een formaliteit inhoudt en onvoldoende basis biedt voor toezicht op verwerkingen, uitvoering geven aan rechten betrokkene of bijdragen aan werkprocessen.
Niettemin moet worden geconstateerd dat het register van de gemeente en de BAR-organisatie op onderdelen meer gedetailleerd verwerkingen beschrijft dan dat van – bijvoorbeeld – de AP zélf[4]. Hierdoor lijkt het door de gemeente gehanteerde register in ieder geval te voldoen aan de eisen die in het Nederlands bestel aan een dergelijk register worden gesteld.

DPIA (Data Protection Impact Assessment)

Op grond van artikel 35 AVG is de BAR-organisatie verplicht een DPIA (Gegevensbeschermingseffectbeoordeling) te laten uitvoeren.

Informatiebeveiligingsmaatregelen zijn altijd “risk based”, proportioneel en gebaseerd op een zorgvuldige afweging, een dataclassificatie, daar waar wettelijke verplicht of gewenst een Privacy Impact Assessment (gegevensbeschermingseffectbeoordeling) en een risicoanalyse.

Een DPIA geeft inzage in de verwerkingsrisico’s en geeft **geen opsomming van de maatregelen** die het risico kunnen afdekken. Op basis van de uitkomsten van de DPIA zullen de PO en CISO het lijnmanagent (proceseigenaar) adviseren over welke maatregelen de risico’s kunnen afdekken. Uiteindelijk zullen de maatregelen in het rapport van de DPIA worden meegenomen en dan moeten ook nog de restrisico’s worden benoemd in het rapport. De AP heeft een lijst van verwerkingen gepubliceerd waarvoor verplicht een DPIA moet worden uitgevoerd.

[4] Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verwerkingsregister_ap.pdf.

Ook als een DPIA niet verplicht is, is het uitvoeren van een (gedeeltelijke) DPIA raadzaam bij een (nieuwe) gegevensverwerking. Men spreekt in een dergelijk geval van een 'DPIA-light' of een 'Privacy Quick Scan'. Organisaties kunnen op deze manier ook voor deze verwerkingen de privacy risico's in kaart brengen en mitigeren. Een "DPIA-light" of "Privacy Quick Scan" draagt bij aan de aantoonbaarheid van compliance maatregelen.

Dpia's worden in de BAR-organisatie niet structureel uitgevoerd. In de praktijk gaat er veel tijd zitten in controles en adviezen rond DPIA. In de interviewgesprekken wordt gemeld dat er soms ook weerstand op afdelingen is, omdat het als extra werk wordt gezien. Hier is frictie zichtbaar in wat in de praktijk wordt uitgevoerd en wat de AVG als wettelijke eis aan de organisatie stelt. Bovendien stelt de FG, heeft de organisatie nog geen uniforme procedure voor het uitvoeren van een DPIA. Er wordt in de praktijk niet vastgelegd wanneer en waarom daarvan wordt afgeweken. Eventuele beveiligingsrisico's die daardoor al dan niet (impliciet) worden genomen worden niet gedocumenteerd in een besluitvormingsdocument.

Er is binnen NARIS (risicobeheersprogramma) een DPIA ingericht. De PO en CISO voeren samen met de domeindeskundigen (applicatiebeheerder/kwaliteitsmedewerker/enz.) deze DPIA uit. Vanuit NARIS wordt een rapportage gegenereerd. Op basis van de uitkomsten van de DPIA stellen de PO en CISO een advies op voor de lijnmanager (proceseigenaar). Eventuele beveiligings/privacy risico's die al dan niet (impliciet) door de lijnmanager worden genomen worden niet gedocumenteerd in een besluitvormingsdocument.

De reactie van de CISO op het bovenstaande is:
In het nieuwe beveiligingsbeleid dat binnenkort wordt vastgesteld en BIO proof is (Baseline informatieveiligheid overheid) staat in de paragraaf beleidsuitgangspunten:
De te treffen en onderhouden informatiebeveiligingsmaatregelen zijn altijd op een risicoafweging gebaseerd en worden proportioneel getroffen. Deze afweging(en) worden schriftelijk vastgelegd. Een dataclassificatie, **Data Protection Impact Assessment (DPIA)** en een risicoanalyse worden daartoe verplicht uitgevoerd;

Governance (intern extern)

Intern:
Er zijn intern 3 medewerkers actief die zich bezig houden met alles op het gebied van Privacy en Informatieveiligheid. Hieronder wordt de functie genoemd en de taak die bij de functie hoort.

Functionaris Gegevensbescherming (FG)
Deze functionaris is binnen de BAR-organisatie en de drie gemeenten verantwoordelijk voor het toezicht op en advies over de naleving van de AVG, zoals:

- Het toezien op en adviseren over de naleving van wet- en regelgeving en intern beleid omtrent gegevensbescherming.
- Het rechtstreeks rapporteren aan het college van B & W en daar waar de beslissingen genomen worden.
- Het geven van advies met betrekking tot de DPIA en het toezien of de uitvoering daarvan in overeenstemming is met de AVG.

De BAR-organisatie heeft een FG (0,2 fte) ingehuurd en formatief geplaatst op de afdeling Concerncontrol. Deze medewerker treedt onafhankelijk op, adviseert over vraagstukken die in de organisatie spelen ten aanzien van gegevensbescherming, maar mag niet uitvoerend optreden. Bij calamiteiten is deze medewerker de contactpersoon richting de AP. Het contract van deze medewerker is zodanig ingestoken dat het steeds voor 1 jaar wordt verlengd, er ruimte is om bij calamiteiten buiten de 0,2 fte op te treden en bij afwezigheid/verlof een vervanger kan worden aangewezen. Gelet op de grootte van de organisatie en de complexe en langdurige aandachtspunten die in de organisatie liggen is 0,2 fte beslist onvoldoende om een toezichtstaak uit te voeren. De FG is daarom met name met de adviserende rol bezig en probeert dit steeds meer los te laten om richting toezicht te gaan. Bovendien heeft 'BAR 2020' ervoor gezorgd dat de FG het eigen plan van aanpak voor toezicht niet heeft kunnen uitvoeren om op cluster Maatschappij en veiligheid toezicht te houden. Toezicht zonder het opvolgen van de adviezen heeft weinig nut.

Chief Information Security Officer (CISO)
Deze functionaris (1fte) is binnen de BAR-organisatie en de drie gemeenten verantwoordelijk voor alles wat te maken heeft met informatieveiligheid. Beveiliging van informatie en cybersecurity zoals:

- Het geven van gevraagd en ongevraagd advies aan bestuur of management van de organisatie ten aanzien van informatiebeveiliging.
- Verantwoordelijk voor het concern breed beleid, de coördinatie, advisering en rapportage over een samenhangend pakket aan maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening te waarborgen.
- Coördinator verantwoordingsproces voor informatieveiligheid ENSIA (Eenduidige Normatiek Single Information Audit).
- Voorzitter van het interne CERT (Computer Emergency Response Team)
- Het uitvoeren of initiëren van risicoanalyses en interne audits.
- Het coördineren van de werkzaamheden van personen, afdelingen en instanties die betrokken zijn bij de uitvoering van het informatiebeveiligingsbeleid en de daarbij behorende specifieke normenkaders.

Privacy Officer (PO)
Deze functionaris (1fte) is binnen de BAR-organisatie en de drie gemeenten verantwoordelijk voor het adviseren over de te implementeren maatregelen ten behoeve van de AVG zoals:

- Beoordelen of gewerkt wordt conform AVG
- Opstellen privacybeleid
- Adviseren in privacy zaken
- Beoordelen verwerkersovereenkomsten
- Sturen op naleving AVG
- Bewustwording
- Uitvoeren DPIA's

Deze lijst is niet limitatief en komt neer op alle privacy zaken die uitvoering betreffen en de juridische beoordeling daarvan.

Team Informatiebeveiliging en Privacy (TIP)
De medewerkers van dit team komen 1 x per 2 weken bijeen en nemen deel aan het TIP (Team informatiebeveiliging en Privacy). De kern van het TIP bestaat uit de clustermanager Informatisering en Automatisering (I&A), de CISO, de PO en ondersteuning van het bestuurssecretariaat. Daarnaast zijn er nog diverse agendaleden, uit verschillende disciplines zoals architectuur, A-advies, I-advies of Concerncontrol. De FG schuift regelmatig aan. Het TIP heeft tot nu toe gediend als een overlegplatform waar actuele onderwerpen in de organisatie omtrent informatiebeveiliging en privacy zijn besproken, acties zijn uitgezet en acties zijn bewaakt. Deze acties betroffen met name de basis op orde wat betreft de implementatie AVG en de BIO/BIG op orde te krijgen. Momenteel is er behoefte aan goede positionering van het TIP in de organisatie, beschrijving van taken en bevoegdheden en eventueel toekenning financiële middelen. Vanuit het TIP wordt een directievoorstel voorbereid om TIP beter te positioneren in de organisatie.

Governance Extern:
<u>Verwerkingsovereenkomsten:</u>
Op grond van artikel 28 AVG is de BAR-organisatie verplicht een verwerkingsovereenkomst te sluiten met organisaties die werkzaamheden verrichten voor de BAR-organisatie, waarin persoonsgegevens worden verwerkt. In deze overeenkomst wordt afgesproken hoe deze externe verwerker omgaat met de persoonsgegevens van de gemeente in de uitvoering van de uitbestede taken. Bijvoorbeeld hoe de persoonsgegevens opgeslagen en beveiligd moeten worden, met wie ze worden gedeeld en hoe lang de gegevens worden bewaard.

In de praktijk is het overeenkomen van een verwerkingsovereenkomst een lastig vraagstuk, omdat veel organisaties niet kunnen of willen voldoen aan beveiligingseisen die de BAR-organisatie op basis van de AVG (o.a. art 32 AVG) en het informatiebeveiligingsbeleid aan de verwerking van de persoonsgegevens stelt. In een interviewgesprek werd als voorbeeld genoemd:

“Bij de aanbesteding van kopieerapparaten was de eis gesteld dat de leverancier garanties moest geven dat gegevens van de kopieermachines niet op straat zouden belanden”. Uiteindelijk, met veel moeite lukte het om één organisatie te vinden die aan de eis kon voldoen. Het probleem ligt in het niet akkoord willen gaan met de beveiligingseisen die wij volgens ons informatiebeveiligingsbeleid, de DPIA en risicoanalyse stellen en daardoor gaan de partijen niet akkoord met een verwerkingsovereenkomst.
Een andere oorzaak is dat reeds inkoopafspraken zijn gemaakt met de leverancier en de diensten worden afgenomen en later aan een verwerkersovereenkomst wordt gedacht. Deze (inkoop)afspraken zijn dan gemaakt zonder de PO en CISO vooraf om advies te vragen, waardoor de informatiebeveiligingseisen en privacy eisen niet zijn meegenomen in het pakket van eisen. Dit brengt de organisatie dan in een minder sterke onderhandelingspositie om een verwerker volgens de eisen van de gemeente te laten werken en dit in een verwerkersovereenkomst vastgelegd te krijgen.
De gemeente Albrandswaard heeft wettelijke taken, waarvan een deel door externe partijen wordt uitgevoerd en als deze partijen niet willen of kunnen voldoen aan de eisen die de gemeente stelt en daardoor het erg lang duurt voordat er een verwerkingsovereenkomst is gesloten, is voor de gemeente Albrandswaard erg lastig om de wettelijke taken volgens de vereisten van de AVG uit te voeren.
Dit gegeven maakt dat de gemeente Albrandswaard hierin het maximaal mogelijke doet om op dit punt aan de eisen van de AVG te voldoen. Een risico zal geaccepteerd moeten worden omdat de kans bestaat dat meer inspanning op dit punt disproportioneel is. Deze beveiligings/privacy risico’s worden al dan niet (impliciet) door de lijnmanager genomen en worden niet gedocumenteerd in een besluitvormingsdocument.

De contractmanager van de afdeling inkoop houdt de contracten centraal bij in een applicatie. De clusters en medewerkers geven de getekende contracten door aan inkoop zodat het in de applicatie terechtkomt.
Op dit moment wordt ingestoken op een volledig correcte registratie van verwerkingsovereenkomsten in de wetenschap dat de al bekende informatie niet 100% volledig is. De verwachting is dat dit zich in de toekomst vanzelf oplost, omdat de bestaande contracten binnen 4 jaar zijn afgelopen. De vraag is of deze verwachting klopt omdat er ook contracten zijn voor onbepaalde tijd**.**

3.3 Informatiebeveiliging

De drie gemeenten hebben via de BAR-organisatie vanaf 2015 een CISO in dienst waardoor op het gebied van informatieveiligheid en automatisering veel zaken beleidsmatig op orde zijn gebracht. De CISO heeft tijdens het interview aangegeven dat de meeste applicatiebeheerders en kwaliteitsmedewerkers niet op de hoogte zijn van de/hun verantwoordelijkheden op het gebied van informatieveiligheid en privacybescherming of niet weten dat ze voor de CISO/PO/FG het eerste aanspreekpunt zijn. Hiervoor is ook geen tijd vrij gemaakt binnen hun werkzaamheden. De CISO heeft tevens aangegeven dat hierdoor de uitvoering van de kerntaken door de CISO (die verantwoordelijk is voor concern breed beleid, coördinatie, advisering en rapportage) onder druk staan, omdat de CISO wordt ingezet/betrokken bij de uitvoerende taken die eigenlijk zelfstandig door de afdelingen moeten worden uitgevoerd.

In het nieuwe beveiligingsbeleid is opgenomen in de paragraaf 3.4: Verantwoordelijkheden van de proceseigenaar (lijnmanager)

Het beveiligen van gegevens (data) en de informatiesystemen is geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. De noodzaak, aard en omvang van de informatieveiligheid is binnen ieder vakgebied anders. Zo heeft ieder proces te maken met een eigen informatievoorziening en eisen die volgen uit (sectorale) wet- en regelgeving. **De proceseigenaar (lijnmanagement) is verantwoordelijk voor de implementatie en het in stand houden van de informatieveiligheid en de bijbehorende informatiebeveiligingsmaatregelen binnen:**

1. Het betrokken organisatieonderdeel en de processen;
2. De bijbehorende informatiesystemen (applicaties, procedures, enzovoorts), inclusief informatiesystemen die in de Cloud zijn ondergebracht;
3. De gegevensverzamelingen, inclusief gegevensverwerkingen (data) die in de Cloud zijn ondergebracht;

Daarnaast is proceseigenaar (lijnmanagement) verantwoordelijk voor de periodieke rapportage over de status van de informatieveiligheid binnen zijn of haar organisatieonderdeel en processen aan de Chief Information Security Officer;

De hackaanvallen worden steeds complexer waardoor er voldoende expertise nodig is om de digitale aanvallen te kunnen weerstaan.
De praktijk is dat hackaanvallen vaker voorkomen en dit vormt een bedreiging voor de continuïteit van de bedrijfsvoering. Cybercriminaliteit heeft de laatste jaren een grote vlucht genomen en geen enkele overheidsorganisatie ontkomt aan pogingen van onbevoegden om informatie buit te maken of om de bedrijfsvoering te verstoren. Cybercriminaliteit is inmiddels “big business” en een serieus verdienmodel voor criminelen. Daarmee is een permanente wedloop ontstaan tussen beveiligingsmaatregelen en innovatie in het hacken van organisaties. Helaas betreft het voorkomen van onrechtmatige toegang (cyberaanvallen en hacking) tot onze gegevens en het treffen van passende beveiligingsmaatregelen een bewegend doel, waardoor we nooit “klaar” zijn. De dreigingen, kwetsbaarheden en technische mogelijkheden veranderen namelijk constant.

Een voorbeeld”:
Op 6 juni 2019 ontdekte de gemeente Lochem dat haar ICT-systeem gehackt was. Uit hun aanpak blijkt dat de dader(s) heel geraffineerd te werk zijn gegaan. De aanval was erop gericht grote delen van de administratie te versleutelen en losgeld te eisen. Van een datalek van bedrijfsgegevens is melding gemaakt bij de Autoriteit Persoonsgegevens. De gemeente Lochem heeft beveiligingsexpert Brenno de Winter gevraagd te assisteren bij het bestrijden van de crisis en een duidingsrapportage te schrijven. Hij concludeert dat Lochem ‘door het oog van de naald is gekropen’, omdat het versleutelen van gegevens tonnen schade had kunnen veroorzaken.

De CISO wijst op de mogelijkheid (noodzaak in verband met de benodigde expertise) van het abonneren op Security Operations Center (SOC). Dit is een onderdeel binnen de GGI veilig [5] aanbesteding.
Dit is een organisatie die tegen betaling (abonnementsvormen) de digitale systemen van de BAR-organisatie 24 uur per dag bewaakt en melding maakt van bedreigingen als hacken aan de orde is of als serieuze kwetsbaarheden worden ontdekt. Voor de opvolging/afhandeling van de melding die vanuit het SOC komen is extra FTE en specifieke kennis nodig.
Zo zijn er meer mogelijkheden om de digitale weerbaarheid van de gemeente te verhogen.

De CISO heeft in het interviewgesprek de volgende aandachtspunten genoemd en er aandacht voor gevraagd:

a. Stel een duidelijk structuur op over wat we doen als zich een hackaanval voordoet. Taken en bevoegdheden. En een communicatiestructuur. Regel de business continuïteit. Welke bedrijfsvoering processen hebben prioriteit en in welke volgorde moeten ze weer beschikbaar komen.
b. Er is nu wel een technisch draaiboek (om de techniek in de lucht te brengen), maar er is geen operationeel draaiboek waarin staat hoe we de bedrijfsprocessen gaan uitvoeren, in welke volgorde en waar? Zorg voor een operationeel draaiboek.
c. Zorg voor Forensische ondersteuning in de vorm van een abonnement of contract op ICT-gebied om onderzoek te kunnen doen in het geval van een hack waardoor onze digitale systemen niet meer beschikbaar zijn of bij een groot datalek.
d. Zorg voor een crisis draaiboek.

In het kader van dit onderzoek is informatiebeveiliging globaal aan de orde gesteld (zie onderzoek aanpak).
Uit het bovenstaande blijkt wel dat nader onderzoek op het gebied van risico’s bij informatieveiligheid gewenst is met name als het gaat om business continuïteit. Aanbevolen wordt de voortgang van knelpunten op het gebied van informatieveiligheid frequenter op de agenda van de directieraad te plaatsen.

[5] https://www.vngrealisatie.nl/producten/ggi-veilig

Bewustwording:
De stappen om bewustwording van informatiebeveiliging en privacybescherming binnen de organisatie op niveau te houden worden op basis van risico, actualiteit en behoefte van de klant uitgevoerd. Zo wordt er op basis van risico-analyses met risicovolle clusters/teams gesproken. Met posters in de lift wordt opgeroepen zorgvuldig met gegevens om te gaan. Ook op het computerscherm van de medewerkers wordt informatie gegeven over aandacht voor privacy en informatiebeveiliging, zoals onder andere “sluit je scherm af als je de kamer verlaat, beveilig je wachtwoorden”. Er is echter geen vastgesteld bewustwordingsprogramma met een bijbehorende planning en Plan-Do-Check-Act-cyclus.

3.4 De AVG binnen cluster Maatschappij

Binnen dit cluster wordt veelvuldig met persoonsgegevens gewerkt. Gezien de omvang van dit cluster en de aard van de werkzaamheden (veel processen met persoonsgegevens) die daar worden verricht, komt uit diverse interviewgesprekken naar voren dat er sterk de behoefte bestaat om bij dit cluster een “eigen privacy specialist” en informatiebeveiligingsspecialist aan te stellen.
Deze rol ligt nu bij kwaliteitsmedewerkers van dit cluster maar, wordt gemeld in een interview, deze medewerkers zijn overbelast door een hoge werkdruk. Het voldoen aan de eisen die de AVG stelt, staat hierdoor in de werkprocessen van dit domein, onder druk.
Van oktober 2019 t/m januari 2020 is door cluster Maatschappij tijdelijk extern een privacy adviseur ingehuurd, die een bijdrage heeft geleverd aan de borging van de privacy in de processen, waarbij het de inzet is om integraal werken binnen de wettelijke kaders mogelijk te maken. Door hem is geconstateerd dat er nog veel werkzaamheden op het gebied van privacy in processen en de cultuur van de organisatie uitgevoerd moeten worden. Deze externe adviseur heeft onder andere gewerkt aan een DPIA om de grondslagen en risico’s bij integraal werken binnen het cluster Maatschappij in beeld te brengen. Met de medewerkers van dit cluster wordt nu door de PO van de BAR-organisatie gekeken naar de scope van een dergelijke toets en of het mogelijk is om dit in één keer in zijn geheel te toetsen.
Door het management van het cluster Maatschappij is besloten om de implementatie van de BIO in 2019 niet uit te voeren en uit te stellen, omdat medewerkers maar één keer tegelijkertijd belast kunnen worden. Het management van het cluster Maatschappij heeft geen duidelijkheid verschaft over hoe en wanneer de implementatie van de BIO wel zal plaatsvinden. Het niet implementeren van de BIO vormt binnen het Sociaal Domein een risico, omdat daar veelal risicovolle gegevensverwerkingen plaatsvinden.

3.5 Verantwoording

Zoals in hoofdstuk 3.1 is beschreven is het informatieveiligheidsbeleid en het privacy beleid formeel vastgesteld en worden AVG-maatregelen in de organisatie ook uitgevoerd.

De gemeenteraad van Albrandswaard heeft op 7 oktober 2019 het Privacy beleid 2019/2020 vastgesteld. Daarmee is de laatste stap genomen in het traject om dit beleid vast te stellen. Het beleid is inmiddels bekendgemaakt via de afzonderlijke gemeentebladen en daarmee in werking getreden en is verantwoording afgelegd over het borgen van de naleving van de AVG binnen de organisatie.

Met deze vaststelling en bekendmaking zijn nu alle gemeenten – en daarmee ook de BAR-organisatie zelf – voorzien van een beleidskader rond de AVG.

4 Samenvatting conclusie en aanbevelingen

4.1 Samenvatting

In hoofdstuk 3.1 is kort het beleid beschreven en de resultaten die dit beleid heeft opgeleverd. In diverse interviewgesprekken is gewezen op de tijd die het kost om aan de verplichtingen van de AVG te voldoen. Dit heeft geleid tot de aanbeveling om de kosten hiervan structureel in de begroting p te nemen. In hoofdstuk 3.2 is de uitvoering van het beleid kort beschreven. Met name het verwerkingsregister was hierin een aandachtspunt. De FG heeft hierover een aanbeveling gedaan. In hoofdstuk 3.3 zijn de rollen van de Privacy medewerkers beschreven en is aangegeven hoe de taken in de organisatie zijn belegd. In hoofdstuk 3.3 is ook de Governance extern beschreven en heeft de FG met name over het verwerkingsregister een aanbeveling gedaan.
In hoofdstuk 3.4 zijn de risico's omtrent informatiebeveiliging kort uitgewerkt. Uit de interviewgesprekken met de Privacy medewerkers wordt aangegeven dat hack-aanvallen steeds complexer worden en er diverse knelpunten zijn waarvoor aandacht nodig is. In diverse interviewgesprekken is gewezen op informatieveiligheid binnen cluster Maatschappij. In hoofdstuk 3.4 is hiervan een korte samenvatting gegeven.
In hoofdstuk 3.5 is kort de wijze van verantwoording van de AVG door de gemeente beschreven. De diverse stappen die nodig zijn om aan de eisen van de AVG in de gemeentelijke organisatie te voldoen zijn in de aanbevelingen opgenomen.

4.2 Conclusie

De BAR-organisatie heeft een groot aantal maatregelen genomen om te voldoen aan de AVG-eisen en is daarin op de goede weg, maar nog niet alle maatregelen van het 10-stappenplan van de Autoriteit Persoonsgegevens zijn volledig ingevoerd. Dit houdt in dat nog niet volledig is voldaan aan de "formele eisen" van de AVG.

Geconcludeerd wordt dat de uitvoering van de AVG-complex en veelomvattend is. Er zijn veel wettelijke regels en bepalingen en in de praktijk is de relatief jonge AVG nog niet volledig geland en "tussen de oren".
Naast het gegeven dat gegevensbescherming altijd al een belangrijk item is geweest, heeft dit onderwerp in de huidige digitale wereld nieuwe prioriteit gekregen. Dit is wennen en blijft aandacht vragen in de cultuur en soft skills van de gemeentelijke organisatie. Achtereenvolgens zijn de volgende 10 conclusies getrokken. Vervolgens zijn hierop 10 aanbevelingen gedaan:

1. Vastgesteld is dat niet inzichtelijk is wat de kosten van de implementatie en naleving van de AVG voor de gemeente Albrandswaard zijn omdat de diverse activiteiten die betrekking hebben op AVG-maatregelen, verspreid zijn over verschillende werkzaamheden van medewerkers binnen de BAR-organisatie.

2. De FG heeft opgemerkt dat de formatie (0,2fte) niet voldoende is om de toezichthoudende taken uit te voeren. Ook heeft de FG opgemerkt dat de ondersteuning van het cluster Maatschappij niet voldoende is om de AVG-eisen in dit cluster ingebed te krijgen.

3. Er is behoefte aan een goede positionering van het team TIP (Team informatiebeveiliging en Privacy) in de organisatie, een beschrijving van taken en bevoegdheden en het toekennen van financiële middelen.

4. De (voormalige) FG gaf aan dat er wel een verwerkingsregister is maar dat deze er vooral is om aan de eisen te voldoen. Het register wordt niet regelmatig bijgehouden, is daardoor niet compleet, en vanwege de zeer algemene opstelling niet bruikbaar voor de organisatie om beter in control te zijn.

5. Binnen het cluster Maatschappij wordt veelvuldig met persoonsgegevens gewerkt. Gezien de omvang van dit cluster en de aard van de werkzaamheden (veel processen met persoonsgegevens) die daar worden verricht, is het risico op het niet voldoen aan de AVG-eisen hoog.
   Door het management van het cluster Maatschappij is besloten om de implementatie van de BIO (Baseline informatiebeveiliging Overheid) in 2019 niet uit te voeren en uit te stellen, omdat medewerkers maar één

keer tegelijkertijd belast kunnen worden. Het management van het cluster Maatschappij heeft geen duidelijkheid verschaft over hoe en wanneer de implementatie van de BIO wel zal plaatsvinden. Het niet implementeren van de BIO vormt binnen het Sociaal Domein een risico, omdat daar veelal risicovolle gegevensverwerkingen plaatsvinden.

6. Aan verwerkingsovereenkomsten wordt veel aandacht besteed. De belemmeringen liggen vaak bij leveranciers die niet aan de eisen die worden gesteld door de gemeente Albrandswaard op het gebied van privacy, kunnen voldoen. Dit komt ook omdat de eisen vaak niet vooraf worden gesteld omdat de PO en CISO pas achteraf worden betrokken.
7. Uit het onderzoek naar informatieveiligheid blijkt dat nader onderzoek op het gebied van risico's bij informatieveiligheid gewenst is. In de bedrijfsvoeringskant ontbreekt een business continuïteitsplan, technische mogelijkheden zijn beschikbaar. Aanbevolen wordt dat de voortgang van knelpunten omtrent informatieveiligheid frequenter op de agenda van de directieraad komen te staan.
8. Vastgesteld is dat de stappen om bewustwording van informatiebeveiliging binnen de organisatie op niveau te houden ad hoc worden uitgevoerd. Er is geen vastgesteld bewustwordingsprogramma met een bijbehorende planning en Plan-Do-Check-Act-cyclus.

4.3 Aanbevelingen

1. Maak de kosten van de naleving van de AVG zichtbaar door het hoofd informatiemanagement te verzoeken een financieel overzicht te bouwen waarin de verschillende kosten onder elkaar worden gezet en gerapporteerd.
2. Zorg dat de FG in samenspraak met de CISO en de PO over 6 maanden vaststelt, hoeveel formatie er nodig is om de AVG taken en toezichthoudende taken uit te voeren.
3. Zorg voor een goede positionering van het team TIP (Team informatiebeveiliging en Privacy)
4. Zorg dat het verwerkingsregister aantoonbaar volledig is ingevuld en zorg voor een procedure waarin wijzigingen in processen worden gemeld aan de beheerder van het verwerkingsregister.
5. Zorg voor structurele ondersteuning van de AVG en informatieveiligheid (implementatie BIO) binnen het cluster Maatschappij en maak hiervoor structureel financiële middelen beschikbaar. Maak het mogelijk dat cluster Maatschappij in staat is om de BIO in te voeren. (Baseline informatiebeveiliging Overheid)
6. Zorg er voor dat verwerkingsovereenkomsten en de eisen tav informatieveiligheid en privacybescherming in het pakket van eisen vooraf aan de aanbesteding/aankoop goed geborgd zijn bij de inkoopactiviteiten. De verwerkingsovereenkomst dient vooraf te worden afgesloten en niet achteraf. Zorg voor een procedure verwerkingsovereenkomsten waarin de stappen worden uitgelegd en waarin ook de risico's beschreven zijn.
7. Zorg voor een BCM (Business continuity management) met duidelijke governance en processtappen, waarbij de processen erop gericht zijn de uitval van systemen te voorkomen en in het geval van uitval de herstelprocessen de hoogste prioriteit hebben. Daarbij wordt aanbevolen dat de voortgang van knelpunten frequenter op de agenda van de directieraad komen te staan.
8. Zorg voor een vastgesteld meerjaren AVG en informatieveiligheids-bewustwordingsprogramma met een bijbehorende planning en PDCA- cyclus (Plan Do Check Act cyclus) en neem dit op in de begroting.

De vakafdeling heeft kennis genomen van de conclusies en aanbevelingen uit dit rapport:
De nadere uitwerking van de aanbevelingen vindt plaats binnen het programma Informatieveiligheid en Privacy. Een jaarplan wordt opgesteld met inzicht in de te behalen doelen, de risico's die al dan niet worden afgedekt en de daarbij benodigde capaciteit en financiële middelen. Op basis van scenario's kunnen structurele keuzes worden gemaakt.

4.4 Bijlagen:

1 10-stappenplan AP

2 Privacy beleid

3 Informatiebeveiligingsbeleid.

AUTORITEIT
PERSOONSGEGEVENS

In 10 stappen voorbereid op de AVG

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?

De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

Wat kan ik doen?

Als organisatie kunt u nu alvast stappen ondernemen om straks klaar te zijn voor de AVG. Om u hierbij te helpen, heeft de Autoriteit Persoonsgegevens de 10 belangrijkste stappen voor u op een rijtje gezet. Op autoriteitpersoonsgegevens.nl vindt u de antwoorden op veelgestelde vragen.

Stap 1: Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven, zoals guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.

Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Bereid u daar op voor zodat u op tijd en op de juiste manier op verzoeken reageert.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Stap 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt. Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt.

U kunt het overzicht ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Vermeld in het overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag u deze gegevens verwerkt. Beroept u zich bijvoorbeeld op een gerechtvaardigd belang of vraagt u toestemming aan de betrokkenen? NB: de grondslagen in de AVG zijn grotendeels hetzelfde als die in de huidige Wbp.

Stap 4: Data protection impact assessment

Onder de AVG kunt u verplicht zijn een zogeheten *data protection impact assessment* (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt straks uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

Stap 5: Privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design* en *privacy by default* en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;

- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

Stap 6: Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

Stap 7: Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Stap 8: Bewerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Stap 9: Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

Stap 10: Toestemming

Voor sommige gegevensverwerkingen hebt u toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

Informatiebeveiligingsbeleid

Gemeente Albrandswaard

INFORMATIEVEILIGHEIDSBEWUSTZIJN IS DE BELANGRIJKSTE BEVEILIGINGSMAATREGEL

COLOFON

NAAM DOCUMENT

Informatiebeveiligingsbeleid gemeente Albrandswaard

NUMMER ZAAKSYSTEEM

116727

DOEL EN SCOPE INFORMATIEBEVEILIGINGSBELEID

Dit Informatiebeveiligingsbeleid is er op gericht hoe binnen de gemeente Albrandswaard met informatieveiligheid omgegaan moet worden en bevat de beleidsuitgangspunten voor de verdere implementatie. In dit informatiebeveiligingsbeleid wordt uitgewerkt wat:

1. De verantwoordelijkheden zijn van:
    a. Het college van burgemeester en wethouders;
    b. De directieraad van de BAR-organisatie en de directie van NV BAR-afvalbeheer;
    c. De Chief Information Security Officer (CISO);
    d. De proceseigenaar (lijnmanagent);
    e. Medewerkers, (keten)partners en belanghebbende(n).
2. De beleidsuitgangspunten zijn;
3. De wijze is waarop het beschermingsniveau wordt vastgesteld.
4. Het doel van informatieveiligheid is.

Door organisatorische, juridische, technische en fysieke informatiebeveiligingsmaatregelen te treffen en te onderhouden is de gemeente Albrandswaard in staat om de kwaliteitskenmerken zoals de beschikbaarheid, vertrouwelijkheid en integriteit van haar gegevens (data) te waarborgen. In dit informatiebeveiligingsbeleid wordt beschreven met welke beleidsuitgangspunten de gemeente Albrandswaard rekening dient te houden bij het borgen van de informatieveiligheid. De beleidsuitgangspunten in dit informatiebeveiligingsbeleid gaan uit van de minimale eisen die worden gesteld aan informatiebeveiliging op basis van de Baseline Informatiebeveiliging Overheid[1] (BIO). Informatiebeveiliging vindt plaats conform “best practices” (de stand der techniek), waarbij geldt dat de vereiste informatiebeveiligingsmaatregelen sterker dienen te zijn naarmate gegevens gevoeliger zijn.

DOELGROEP

Dit informatiebeveiligingsbeleid is van toepassing op de gemeente Albrandswaard en alle uit te voeren processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen), inclusief gegevensverwerking die door de gemeente Albrandswaard in de Cloud of bij (keten)partners zijn of worden ondergebracht. Dit informatiebeveiligingsbeleid is openbaar en is beschikbaar voor proceseigenaren (lijnmanagement), applicatiebeheerders, externe partijen, ketenpartners, medewerkers en andere belanghebbende(n).

[1] Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Van BIG, BIR, BIR2017, IBI en BIWA naar BIO. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek.

Dit informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Overheid.

VERSIE

Definitief d.d. 23-06-2020

VERSIEBEHEER

Het beheer van dit document berust bij de Chief Information Security Officer

RELATIE MET ANDERE PRODUCTEN

Dit informatiebeveiligingsbeleid heeft een relatie met:

1. De resolutie informatieveiligheid VNG;
2. Eenduidige Normatiek Single Information Audit (ENSIA);
3. De volgende maatregelen uit de Baseline Informatiebeveiliging Overheid;
    a. Control: 5.1.1;
    b. Control: 5.1.2;
    c. Overheidsmaatregel: 5.1.1.1;
    d. Overheidsmaatregel: 5.1.2.1
4. Overige relevante documenten.

VASTSTELLING EN INWERKINGTREDING

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door het college van Burgemeester en Wethouders van de gemeente Albrandswaard. Hiermee komt het voorgaande (vastgestelde) informatiebeveiligingsbeleid te vervallen. Dit informatiebeveiligingsbeleid werd vastgesteld door:

Het college van Burgemeester en Wethouders van de gemeente Albrandswaard op 30-06-2020.

INHOUD

1: INLEIDING / MANAGEMENTSAMENVATTING

De gemeente Albrandswaard beheert veel gegevens, waaronder (bijzondere) persoonsgegevens, zoals medische- en strafrechtelijke gegevens en gevoelige gegevens, zoals het **B**urger**S**ervice**N**ummer en financiële gegevens. Burgers en bedrijven verwachten van de gemeente Albrandswaard dat de gemeente zorgvuldig omgaat met deze (persoons)gegevens. Hoe gevoeliger/waardevoller deze (persoons)gegevens zijn, hoe meer maatregelen er getroffen en in stand gehouden moeten worden om deze gegevens te beschermen tegen onrechtmatige toegang en/of misbruik en/of manipulatie. Het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van deze (persoons)gegevens en de continuïteit van de dienstverlening van de gemeente Albrandswaard is waar het uiteindelijk om gaat. Dit kan de gemeente Albrandswaard realiseren door het treffen en onderhouden van passende organisatorische, juridische, technische en fysieke informatiebeveiligingsmaatregelen.

2: DOEL VAN HET INFORMATIEBEVEILIGINGSBELEID

Dit informatiebeveiligingsbeleid is er op gericht hoe binnen de gemeente Albrandswaard met informatieveiligheid omgegaan moet worden en bevat de beleidsuitgangspunten voor de verdere implementatie. In dit informatiebeveiligingsbeleid wordt uitgewerkt wat:

1. De verantwoordelijkheden zijn van:
    a. Het college van burgemeester en wethouders;
    b. De directieraad van de BAR-organisatie en de directie van NV BAR-afvalbeheer;
    c. De Chief Information Security Officer (CISO);
    d. De proceseigenaar (lijnmanagent);
    e. Medewerkers, ketenpartners en belanghebbende(n).
2. De beleidsuitgangspunten zijn;
3. De wijze is waarop het beschermingsniveau wordt vastgesteld;
4. Het doel van informatieveiligheid is.

3: VERANTWOORDELIJKHEDEN

3.1: VERANTWOORDELIJKHEDEN VAN HET COLLEGE VAN BURGEMEESTER EN WETHOUDERS

Het college van burgemeester en wethouders van de gemeente Albrandswaard speelt een cruciale rol bij de uitvoering van dit informatiebeveiligingsbeleid. Het college van burgemeester en wethouders van de gemeente Albrandswaard geeft richting aan het informatiebeveiligingsbeleid, bepaalt welke informatiebeveiligingsrisico's acceptabel zijn en welke informatiebeveiligingsrisico's ze wil afdekken. De uitvoering van het informatiebeveiligingsbeleid is belegd bij het bestuur van de BAR-organisatie en de directie van de NV BAR-afvalbeheer. Zij zorgen voor de uitvoering van dit beleid, de implementatie en het onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integri-

teit en vertrouwelijkheid van de informatievoorziening te waarborgen. Het college van burgemeesters en wethouders van de gemeente Albrandswaard houdt hier toezicht op. Daarnaast legt het college van burgemeester en wethouders verantwoording af (aan de landelijke toezichthouders en de gemeenteraad) over de status van de informatieveiligheid binnen de gemeente. Deze verantwoording bestaat uit een jaarlijkse zelfevaluatie (ENSIA[2]), een IT-audit, een verklaring van het college van burgemeester en wethouders (collegeverklaring) en een passage over informatieveiligheid in het jaarverslag.

3.2: Verantwoordelijkheden directieraad BAR-organisatie en de directie van de NV BAR-afvalbeheer

De directieraad van de BAR-organisatie en de directie van de NV BAR-afvalbeheer zijn verantwoordelijk voor het behalen van de gemeentelijke informatiebeveiligingsdoelstellingen. Deze verantwoordelijkheid omvat in elk geval:

1. De implementatie van en het onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen. Dit pakket van samenhangende maatregelen is gebaseerd op een risicoafweging, waarbij het college van burgemeester en wethouders van de gemeente Albrandswaard aangeeft welke informatiebeveiligingsrisico's worden geaccepteerd en welke informatiebeveiligingsrisico's ze door maatregelen willen afdekken/mitigeren;
2. Het opstellen van en uitvoering geven aan het volgende onderliggend beleid:
    a. Cryptografiebeleid;
    b. Logging beleid;
    c. Wachtwoordbeleid;
    d. Clear screen clear desk Beleid.
3. Het inrichten en onderhouden van het proces rondom de verplichte jaarlijkse zelfevaluatie over de status van de informatieveiligheid (ENSIA). Het college van burgemeesters en wethouders van de gemeente Albrandswaard dient hierover jaarlijks aan de landelijke toezichthouders en de gemeenteraad bestuurlijke verantwoording af te leggen. Dit proces omvat minimaal:
    a. Het waarborgen dat aan de auditeisen wordt voldaan;
    b. Het uitvoeren van de zelfevaluatie;
    c. Het laten uitvoeren van een IT-audit door een onafhankelijk en daartoe bevoegd auditor;
    d. Het opstellen en uploaden van de collegeverklaring en het assurance rapport;
    e. Het opstellen en uploaden van de rapportage BRP en Reisdocumenten;
    f. Het opstellen en uploaden van de rapportages BAG, BGT en BRO;
    g. Het afleggen van verantwoording aan het college van burgemeesters en wethouders over de audit resultaten.

[2] ENSIA (Eenduidige Normatiek Single Information Audit).

3.3: VERANTWOORDELIJKHEDEN VAN DE CHIEF INFORMATION SECURITY OFFICER (CISO)

De Chief Information Security Officer zorgt op basis van de Baseline Informatiebeveiliging Overheid concern breed, voor beleid, coördinatie, advisering en rapportage over een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen. De verantwoordelijkheid voor informatieveiligheid, het implementeren en onderhouden van passende informatiebeveiligingsmaatregelen binnen de organisatieonderdelen van de BAR-organisatie en de NV BAR-afvalbeheer ligt evenwel bij de proceseigenaren (lijnmanagers), waarbij het college van burgemeester en wethouders aangeeft welk risiconiveau zij acceptabel vindt of door maatregelen wil afdekken/mitigeren. De Chief Information Security Officer:

1. Rapporteert rechtstreeks aan de gemeentesecretaris van de gemeente Albrandswaard, aan de directieraad van de BAR-organisatie en aan de directie van de NV BAR-afvalbeheer;
2. Heeft periodiek afstemming met de portefeuillehouder binnen het college van burgemeester en wethouders van de gemeente Albrandswaard over de status van de informatieveiligheid;
3. Controleert steekproefsgewijs de naleving van dit informatiebeveiligingsbeleid;
4. Beoordeeld jaarlijks het informatiebeveiligingsbeleid op haar actualiteit en indien nodig wordt dit geactualiseerd;
5. Is de voorzitter van het interne Computer Emergency Response Team (CERT). (Dit is een intern adviesteam voor wat betreft de afhandeling van informatiebeveiligingsincidenten/cyberdreigingen/cyberaanvallen);
6. Is de vertrouwde contactpersoon voor de informatiebeveiligingsdienst (IBD).

3.4: VERANTWOORDELIJKHEDEN VAN DE PROCESEIGENAAR (LIJNMANAGER)

Het beveiligen van gegevens (data) en de informatiesystemen is geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. De noodzaak, aard en omvang van de informatieveiligheid is binnen ieder vakgebied en/of organisatieonderdeel anders. Zo heeft ieder proces te maken met een eigen informatievoorziening en eisen die volgen uit (sectorale) wet- en regelgeving. De proceseigenaar (lijnmanager) is verantwoordelijk voor de implementatie en het in stand houden van de informatieveiligheid en de bijbehorende informatiebeveiligingsmaatregelen binnen:

1. Het betrokken organisatieonderdeel en de processen;
2. De bijbehorende informatiesystemen (applicaties, procedures, enzovoorts), inclusief informatiesystemen die in de Cloud[3] zijn ondergebracht;
3. De gegevensverzamelingen, inclusief gegevensverwerkingen (data) die in de Cloud of bij (keten)partners zijn ondergebracht;

Daarnaast is de proceseigenaar (lijnmanager) verantwoordelijk voor de periodieke rapportage over de status van de informatieveiligheid binnen zijn of haar organisatieonderdeel en processen aan de Chief Information Security Officer;

[3] Cloud computing is het via een netwerk – vaak het internet – op aanvraag beschikbaar stellen van hardware, software en gegevens. Oftewel via het internet verbind je met een server die eender waar kan staan, waarna je alle nodige gegevens (data) en software kan bekijken en gebruiken.

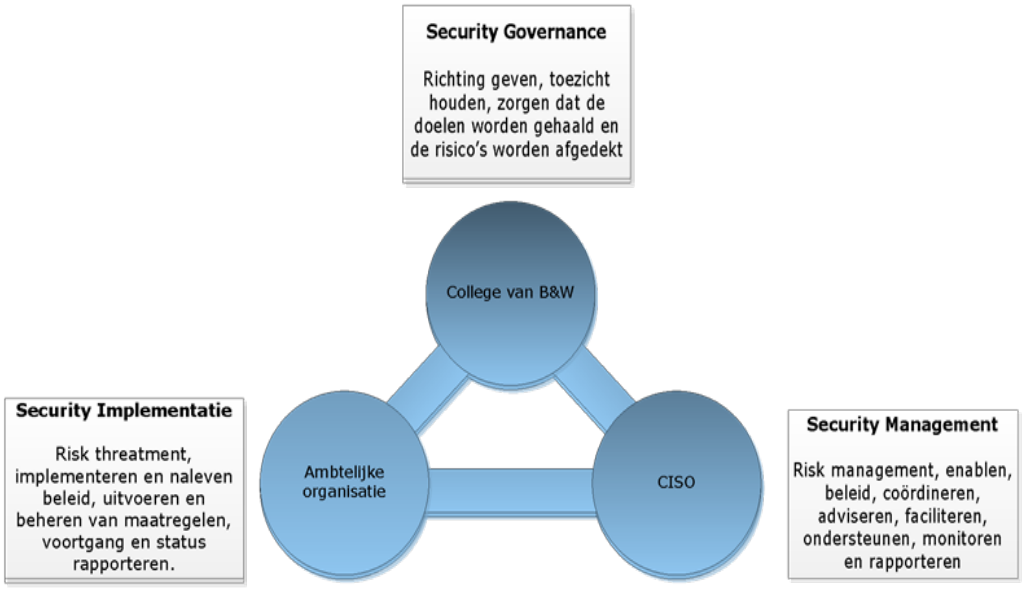
3.5: VERANTWOORDELIJKHEDEN MEDEWERKERS, (KETEN)PARTNERS EN BELANGHEBBENDE(N)

Informatieveiligheid behoort tot de verantwoordelijkheid van alle medewerkers zowel vast als tijdelijk, intern of extern, (keten)partners en andere belanghebbende(n). We gaan daarbij uit van de eigen verantwoordelijkheid voor hun gedrag binnen het vastgestelde beleid, de basisregels en geldende normenkaders. Dit omvat echter altijd:

1. Dat gegevens (data) en applicaties worden beschermd tegen ongeautoriseerde toegang (naleven informatiebeveiligingsbeleid), gebruik, verandering (manipulatie), openbaring, vernietiging, verlies of overdracht;
2. De plicht om (vermeende) informatiebeveiligingsincidenten, zoals datalekken en inbreuken op de informatiebeveiliging via een melding aan de helpdesk te melden;
3. Het aanspreken van in- en externe medewerkers, (keten)partners en betrokkene(n) op geconstateerd onzorgvuldig gedrag in relatie tot informatieveiligheid.

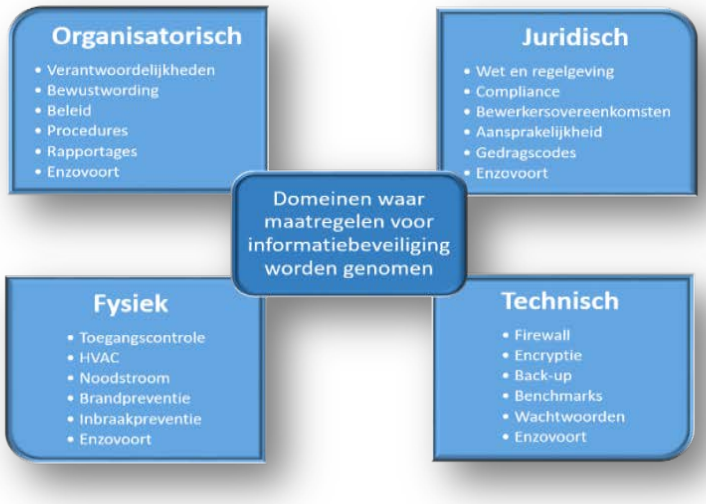
3.6: SCHEMATISCH WEERGAVE VAN DE VERANTWOORDELIJKHEDEN OP HOOFDLIJNEN

Deze verantwoordelijkheden worden hieronder, op hoofdlijnen schematisch weergegeven.



4: DOMEINEN WAAR MAATREGELEN WORDEN GETROFFEN

Om de beschikbaarheid, vertrouwelijkheid en integriteit van de informatievoorziening te waarborgen is het noodzakelijk om een samenhangend pakket van organisatorische, juridische, technische en fysieke informatiebeveiligingsmaatregelen te treffen en te onderhouden. Informatieveiligheid reikt verder dan het implementeren van technische informatiebeveiligingsmaatregelen. Het is een groot misverstand om te denken dat informatiebeveiliging iets technisch is dat centraal geregeld kan of moet worden. Hieronder wordt schematisch weergegeven binnen welke domeinen maatregelen voor informatiebeveiliging worden getroffen en onderhouden. De beschreven maatregelen binnen deze domeinen zijn illustratief en niet limitatief.



5: BELEIDSUITGANGSPUNTEN

Bij het treffen en onderhouden van maatregelen voor de borging van de informatieveiligheid gelden de volgende beleidsuitgangspunten waaraan (vooraf) wordt getoetst:

1. Relevante Europese, landelijke, sectorale wet- en regelgeving en specifieke normenkaders zijn altijd leidend. Denk bij wet- en regelgeving aan de Algemene Verordening Gegevensbescherming (AVG), Wet Basisregistratie Personen (BRP), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de archiefwet, enzovoort;
2. De Baseline Informatiebeveiliging Overheid (BIO) wordt gehanteerd als normenkader. De te treffen informatiebeveiligingsmaatregelen worden hieraan (vooraf) getoetst;
3. De te treffen en onderhouden informatiebeveiligingsmaatregelen zijn altijd op een risicoafweging gebaseerd en worden proportioneel getroffen. Deze afweging(en) worden schriftelijk wordt vastgelegd. Een dataclassificatie, Data Protection Impact Assessment[4] (DPIA) en een risicoanalyse worden daartoe verplicht uitgevoerd;
4. Eventuele (rest) risico's welke niet afgedekt (kunnen) worden met maatregelen of niet proportioneel zijn worden ter acceptatie voorgelegd aan het college van burgemeester en wethouders van de gemeente Albrandswaard;
5. Er is ruimte voor afwijkingen en prioriteringen op basis van het "pas toe of leg uit" principe. Deze afwegingen worden door de proceseigenaar (lijnmanager) schriftelijk vastgelegd, door de Chief Information Security Officer voorzien van een advies en vooraf ter goedkeuring voorgelegd aan de desbetreffende verwerkersverantwoordelijke(n) binnen de gemeente Albrandswaard;
6. Indien van toepassing wordt dit informatiebeveiligingsbeleid verder uitgewerkt c.q. verbijzonderd in onderliggend(e) beleid, informatiebeveiligingsplannen, richtlijnen, procedures, enzovoort. Deze worden getoetst aan de beschikbare operationele producten rondom de Baseline Informatiebeveiliging Overheid;
7. Wanneer wetgeving, regelgeving en/of specifieke normenkaders eisen stellen aan taken en verantwoordelijkheden van medewerkers inzake informatieveiligheid dan

[4] Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

worden deze opgenomen in aanvullende individuele afspraken op functieniveau tussen de leidinggevende en de medewerker. Immers in de HR21 normfuncties zijn de werkzaamheden met betrekking tot informatiebeveiliging niet expliciet opgenomen. Deze specifieke werkzaamheden passen niet bij het karakter van een generieke functiebeschrijving waarin de werkzaamheden op hoofdlijnen zijn beschreven;

8. Iedere medewerker, zowel vast als tijdelijk, intern of extern, (keten)partner of betrokkene, is verplicht waar nodig gegevens en applicaties te beschermen tegen ongeautoriseerde toegang (naleven informatiebeveiligingsbeleid), gebruik, verandering (manipulatie), openbaring, vernietiging, verlies of ongeautoriseerde overdracht. Bij (vermeende) inbreuken hierop dienen medewerkers dit te melden bij de helpdesk;
9. We gaan uit van de eigen verantwoordelijkheid van medewerkers zowel vast als tijdelijk, intern of extern en overige betrokkene(n) voor hun gedrag binnen het vastgestelde beleid, de basisregels en geldende normenkaders;
10. Het college van burgemeester en wethouders van de gemeente Albrandswaard, de directieraad van de BAR-organisatie, de directie van de NV BAR-afvalbeheer, de Chief Information Security Officer en proceseigenaar (lijnmanager) bevorderen de naleving van dit informatiebeveiligingsbeleid, de algehele communicatie en bewustwording (awareness) rondom informatieveiligheid.

6: VERPLICHT UIT TE VOEREN STAPPEN

De te treffen en onderhouden informatiebeveiligingsmaatregelen zijn altijd op een risicoafweging gebaseerd en worden proportioneel getroffen. Om de informatiebeveiligingsrisico's in beeld te brengen en daarmee te komen om een tot een zorgvuldige afweging dienen de hieronder vermelde stappen altijd te worden uitgevoerd. Op basis van deze stappen wordt bepaald wat de te treffen en onderhouden informatiebeveiligingsmaatregelen zijn. Dit wordt schriftelijke vastgelegd.

6.1: HET UITVOEREN VAN EEN DATACLASSIFICATIE (STAP 1)

Het uitvoeren van een dataclassificatie is altijd verplicht. Het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het (vereiste) beschermingsniveau wordt geïdentificeerd. Het vormt de basis voor de basisbeveiligingsniveau-toets (BBN-toets). Het beschermingsniveau van gegevens (data) en/of informatiesystemen wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid. Mede aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. De eerste stap bij een dataclassificatie is nagaan welke wetgeving, regelgeving en/of specifieke normenkaders mogelijk eisen stellen aan gebruik, distributie en opslag van data. Daarnaast is het van belang om de verantwoordelijkheden t.a.v. de gegevens (data) en/of informatiesystemen goed in beeld te hebben. Bij het uitvoeren van een dataclassificatie worden de daarvoor beschikbare operationele producten van de IBD inzake de Baseline Informatiebeveiliging Overheid (BIO) geraadpleegd en als leidraad gehanteerd.

6.2: HET UITVOEREN VAN EEN DATA PROTECTION IMPACT ASSESSMENT (STAP 2)

Een Data Protection Impact Assessment (DPIA) is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en om op basis van de geïdentificeerde risico's de te treffen maatregelen te bepalen om deze risico's af te dekken/mitigeren Het uitvoeren van een Data Protection Impact Assessment (DPIA) is op basis van het beleidsuitgangspunt 3 verplicht en kan in sommige situaties zelfs bij wet[5] verplicht zijn. Bij het uitvoeren van een DPIA worden de daarvoor beschikbare operationele producten van de IBD inzake de Baseline Informatiebeveiliging Overheid (BIO) geraadpleegd en als leidraad gehanteerd.

6.3: UITVOEREN VAN BBN-TOETS EN (DIEPGAANDE) RISICOANALYSE (STAP 3)

De aanpak van onze informatieveiligheid is risico gebaseerd. Dat wil zeggen dat beveiligingsmaatregelen worden getroffen en onderhouden op basis van een (actuele) risicoanalyse en een basisbeveiligingsniveau-toets (BBN-toets). Wanneer de beschikbaarheid en/of integriteit en/of vertrouwelijkheid, of onderdelen van het informatiesysteem een BBN3-niveau behoeft dan dient een aanvullende diepgaande risicoanalyse te worden uitgevoerd. In de overige situaties vormen de uitgevoerde dataclassificatie (stap 1) en het uitgevoerde Data Protection Impact Assessment (DPIA) (stap 2) te samen de risicoanalyse op basis waarvan de te treffen en onderhouden informatiebeveiligingsmaatregelen worden bepaald. Bij het uitvoeren van de BBN-toets en de diepgaande risicoanalyse worden de daarvoor beschikbare operationele producten van de IBD inzake de Baseline Informatiebeveiliging Overheid (BIO) geraadpleegd en als leidraad gehanteerd.

7: HET DOEL VAN HET INFORMATIEVEILIGHEID

Informatiebeveiliging heeft betrekking op het treffen en onderhouden van een samenhangend pakket van maatregelen teneinde de betrouwbaarheid van de informatievoorziening te waarborgen. De informatievoorziening omvat het geheel van beleid, organisatie, procedures, apparatuur, programmatuur, gegevens en mensen dat betrokken is bij de ontwikkeling, implementatie en instandhouding van de informatiehuishouding. Hierbij wordt onderscheid gemaakt tussen beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

7.1: BESCHIKBAARHEID

Beschikbaarheid is het zorgdragen voor het beschikbaar hebben van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor gebruikers. Hierdoor hebben burgers en bedrijven toegang tot voor hen relevante informatie en hebben medewerkers toegang tot relevante informatie om hun werk en de dienstverlening voor onze burgers en bedrijven ongestoord voort te zetten.

7.2: INTEGRITEIT

Integriteit is het waarborgen van de correctheid, volledigheid en tijdigheid (actualiteit) van informatie en informatieverwerking. Voor een efficiënte en effectieve bedrijfsvoering is het

[5] Artikel 35 van de Algemene Verordening Gegevensbescherming (AVG)

voor de gemeente Albrandswaard van belang dat de correcte informatie tijdig aanwezig is in de informatiesystemen en processen.

7.3: VERTROUWELIJKHEID

Vertrouwelijkheid is het beschermen van informatie tegen kennisname, mutatie (manipulatie) en/of verwijderen door onbevoegden. Oftewel informatie is alleen toegankelijk voor degenen die hiertoe zijn geautoriseerd.

7.4: CONTROLEERBAARHEID

De mogelijkheid om vast te kunnen stellen of wordt voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

BIJLAGEN

Geen

Raadsinformatiebrief

De rekenkamer(commissie) van Albrandswaard

Uw brief van:		Ons kenmerk:	211859
Uw kenmerk:		Contact:	H. de Groot
Bijlage(n): 1		Doorkiesnummer:	0180-451594
		E-mailadres:	h.groot@BAR-organisatie.nl
		Datum:	14 oktober 2020

Betreft: Rapport onderzoek AVG Albrandswaard

Geachte heer/mevrouw,

Op basis van artikel 213a van de Gemeentewet heeft de gemeenteraad van Albrandswaard de Verordening onderzoeken doelmatigheid en doeltreffendheid vastgesteld. Deze verordening bepaalt dat het college van B&W periodiek onderzoek doet naar de doelmatigheid en doeltreffendheid van het door het college gevoerde beleid.
Op basis van de verordening hebben wij als college onderzoek laten doen naar de wijze waarop het uitvoeringsproces van de AVG in Albrandswaard is georganiseerd.

Het onderzoeksrapport treft u ter informatie als bijlage bij deze brief aan.

Met vriendelijke groet,

het college van de gemeente Albrandswaard,

de secretaris, de burgemeester,

Hans Cats drs. Jolanda de Witte

BIJLAGEN
1. Het rapport AVG Albrandswaard.