Technische vragen
Raadvoorstel ICT-Beheerplan 2021-2025

Beste,
Hierbij de technische vragen m.b.t het raadsvoorstel ICT-Beheerplan 2021-2025. Dit voorstel komt aan bod tijdens de MR van 24 juni 2021.

Er zijn vragen gesteld over Privacy en Informatiebeveiliging
Op 2 of 9 september wordt er, op voorstel van de agendacommissie, een informatieavond georganiseerd over Privacy en Informatiebeveiliging. De Functionaris gegevensbescherming, de Privacy Officer en de CISO zullen die avond een presentatie verzorgen, waarbij ook voldoende ruimte is voor het stellen van vragen

1. Hoe wordt de ambtelijke organisatie opgeleid om de digitale tools goed te kunnen gebruiken?

Op deze vraag is geen eenduidig antwoord te geven. Digitale tools zijn de afgelopen jaren langzamerhand ingevoerd en niet meer uit ons dagelijks leven weg te denken. Ook in het werk maken wij met name gebruik van digitale tools. Sommigen hiervan werken heel intuïtief door het maken van keuzes via tegels en zijn zonder uitgebreide instructie goed te gebruiken. Voorbeelden hiervan zijn het portal dat medewerkers kunnen gebruiken om hun declaraties in te dienen en Topdesk waarin medewerkers storingen kunnen melden en diverse aanvragen kunnen doen. Via Topdesk is ook een kennissysteem beschikbaar met handleidingen en FAQ's (veelgestelde vragen).
Andere digitale systemen vragen wat meer uitleg. Voorbeelden hiervan zijn de introductie van Teams en OneDrive. Daarvoor zijn organisatiebreed trainingen gegeven. Ook wordt uitleg gegeven aan nieuwe medewerkers over de werking van onze centrale systemen, zoals het financiële systeem en het post en archiefsysteem. Zoals wij hebben aangegeven in het ICT beheerplan worden digitale vaardigheden steeds belangrijker in onze samenleving en daardoor ook binnen de gemeente Nieuwkoop. De verwachting van inwoners en organisaties ten aanzien van digitale oplossingen bij de gemeente nemen toe. Daarnaast dwingt de rijksoverheid met wet- en regelgeving steeds vaker digitalisering af. Om met deze ontwikkelingen mee te kunnen gaan wordt de digitale competentie va onze medewerkers steeds belangrijker. In 2022 starten wij een project waarin wij medewerkers gaan ondersteunen bij het versterken van hun digitale competenties.

2. Welke audits doet de gemeente om te waarborgen dat de AVG nageleefd wordt en de kans op datalekken zo klein mogelijk is?

Op grond van het privacybeleid van de gemeente Nieuwkoop vinden jaarlijks ter controle op de naleving van de AVG auditgesprekken plaats. De audits zijn tot en met 2019 uitgevoerd door een externe auditor in samenwerking met de (toen nog) externe Functionaris gegevensbescherming (FG). Vanaf 2020 doet onze interne FG dit. Met de audit worden de meest risicovolle verwerkingen van persoonsgegevens in de organisatie onderzocht op rechtmatigheid, doelbinding en beschermingsniveau conform de AVG. Uit de audit komen

aanbevelingen voort die erop gericht zijn sturing te geven en een grotere bewustwording te creëren met het doel de kans op datalekken zo klein mogelijk te houden.

3. Hoe ziet het ecosysteem op het gebied van de digitale overheid in de gemeente Nieuwkoop eruit? Menende, waar starten en waar stoppen de verantwoordelijkheden van de gemeente en zijn partners:

    a. Hoe is de verantwoordelijkheid geborgd omtrent de bescherming van persoonsgegevens? Hoe worden deze zaken getoetst? Worden er gegevens van de gemeente op andere plekken opgeslagen? Zo ja, wie is er dan bijvoorbeeld verantwoordelijk voor het beschermen van de persoonsgegevens van inwoners? Is dit alleen de gemeente of wordt deze verantwoordelijkheid soms ook bij partners neergelegd?

De verantwoordelijkheden tussen de gemeente en haar digitale partners omtrent de bescherming van persoonsgegevens zijn vastgelegd in verwerkersovereenkomsten. In deze overeenkomsten is met name vastgelegd welke persoonsgegevens worden gedeeld, welke opdracht hieraan is verbonden, de handelingen die moeten worden verricht als er beveiligingsincidenten of datalekken zijn en dat partijen elkaar medewerking verlenen bij de uitvoering van audits en controles. Het gaat hier om een gedeelde verantwoordelijkheid voor het waarborgen van de veiligheid van de persoonsgegevens van inwoners van de Nieuwkoop. Persoonsgegevens van inwoners worden voor de GBA applicaties opgeslagen op servers in Amsterdam en worden niet gedeeld met bedrijven of subverwerkers die zich buiten Europa of de Europese Economische Ruimte (EER) bevinden.
ICT contracten worden afgesloten op basis van de GIBIT voorwaarden, dit zijn speciale inkoopvoorwaarden voor ICT, ontwikkeld door de VNG.
In deze voorwaarden staat een hoofdstuk opgenomen over verwerking van persoonsgegevens, waarbij de verwerking van persoonsgegevens is geregeld.
O.a. dat persoonsgegevens louter mogen worden opgeslagen binnen de Europese Economisch Ruimte.
Zie voor de GIBIT voorwaarden: https://www.vngrealisatie.nl/sites/default/files/2021-03/GIBIT-2020-Artikelen_0.pdf

    b. Wat is de procedure als er bij de gemeente of een partner van de gemeente een datalek plaatsvind? Wat wordt er gedaan op het moment dat persoonsgegevens van inwoners worden aangetast?

De gemeente hanteert een datalekkenprotocol die wordt gevolgd als er zich bij de gemeente of een partner van de gemeente een datalek voordoet. Als door een datalek gegevens van inwoners zijn betrokken wordt zo spoedig mogelijk actie ondernomen om de oorzaak van het datalek op te sporen, de schade zo beperkt mogelijk te houden en de getroffen inwoners en de Autoriteit Persoonsgegevens indien nodig direct informeren.

4. Tijdens de informatieavond ICT-Beheerplan op 25 mei 2021 werd verteld dat er momenteel ca. 120 applicaties worden gebruikt door de ambtelijke organisatie. Dit lijken er op het oog wat veel. Is het de bedoeling dat deze applicaties in de toekomst allemaal naar de cloud gemigreerd gaan worden?

    a. Zo nee, waarom worden er nog steeds zoveel applicaties gebruikt die lokaal gehost worden terwijl het college een cloudstrategie nastreeft?

In navolging van de cloudstrategie van het College geldt voor elke nieuwe aanvraag in de gemeente Nieuwkoop het uitgangspunt: cloudstrategie, tenzij. En dat tenzij kan dan bijvoorbeeld liggen in onacceptabel hoge kosten of in het feit dat sommige applicaties simpelweg niet als SAAS oplossing worden aangeboden. Elke aanvraag wordt getoetst op eisen die worden gesteld vanuit de Baseline Informatiebeveiliging Overheid. Bij te hoge risico's wordt een cloudapplicatie niet aangeschaft.
Daarnaast worden bestaande contracten nageleefd en dat betekent dat sommige applicaties nog steeds lokaal gehost worden, terwijl ze mogelijk ook al als SAAS oplossing worden aangeboden.

5. Is er een inventarisatie (gedaan) naar de doelmatigheid en doeltreffendheid van deze ca. 120 applicaties en wat zij aan kosten met zich meebrengen voor de gemeente?

Het aantal van 120 applicaties is omvangrijk. Dat hangt uiteraard samen met het omvangrijke takenpakket van gemeenten – en elke taak kent een eigen wijze van uitvoering met eigen digitale ondersteuning. Dit loopt van gladheidsbestrijding tot een kassasysteem bij het zwembad, de beoordeling en uitvoering van WMO-aanvragen, het Geo-domein en nog heel veel meer. Daarnaast is kantoorautomatisering nodig, zodat iedereen het werk goed kan doen. En dan is er ook nog de beveiliging van alle middelen, waarvoor ook meerdere oplossingen worden gebruikt.
In onze applicatie Topdesk staan alle applicaties geregistreerd. De kosten die de applicaties met zich meebrengen zijn opgenomen in het ICT-beheerplan. Alle applicaties worden met enige regelmaat onder de loep genomen, bijvoorbeeld doordat een contract afloopt of door nieuwe wet- en regelgeving waardoor bepaalde taken gaan wijzigen hetgeen doorwerkt in software, et cetera. Voor elke nieuwe aanvraag of voor een wijziging geldt sinds twee jaar dat er een wijzigingsprocedure moet worden doorlopen. Elke wijziging wordt getoetst door het Change Advisory Board (het CAB), waarin adviseurs vanuit informatievoorziening, informatiebeveiliging, gegevensmanagement, technisch ICT-adviseurs en de inkoopadviseur een plek hebben.

6. Heeft de gemeente Nieuwkoop een 'bring your own device'-policy of zijn devices van medewerkers van het ambtelijk apparaat 'van de gemeente'?

Medewerkers werken op een ambtelijk apparaat 'van de gemeente'. Als medewerkers buiten de digitale (Citrix) omgeving van de gemeente Nieuwkoop om, inloggen in een cloudtoepassing, dan krijgen medewerkers uitsluitend toegang met behulp van Multi Factor Authenticatie.

7. Digitale projecten van lokale overheden brengen vaak een grote mate van investeringsonzekerheid met zich mee. Wat doet de gemeente om te voorkomen dat budgetten op ICT overschreden worden?

Ook hier is een deel van het antwoord: de RFC-procedure, waar de inkoopadviseur meekijkt. Daarnaast heeft de gemeente Nieuwkoop besloten de verantwoordelijkheid voor de applicaties die uitsluitend voor de uitvoering van bepaalde gemeentelijke taken worden ingezet, zo laag mogelijk in de organisatie te beleggen. De achterliggende gedachte is dat daar het beste zicht is op wat er nodig is en of een bepaalde toepassing voldoende doelmatig en doeltreffend is. Bewaking van deze uitgaven vind dan ook decentraal plaats.
De verantwoordelijkheid voor de centrale toepassingen is bij Informatisering & Automatisering belegd, waar ook streng wordt toegezien op de beheersing van kosten.

Helaas is niet altijd te voorkomen dat digitale projecten budgetten worden overschreden. Bij de informatieavond over het ICT-Beheerplan op 25 mei j.l. is een toelichting gegeven over ICT en aanbesteden.
Bij een aanbesteding wordt vooraf een programma van Eisen en Wensen opgesteld waar leveranciers op in kunnen schrijven.
Er is bij een aanbesteding een afhankelijkheid van aan aantal factoren, zoals:
- Wie schrijven er in (er zijn ICT leveranciers die afzien van inschrijving vanwege complexiteit die wordt gevraagd, te volle orderportefeuilles, orders aannemen van bedrijfsleven levert meer op, etc.)
- Voor welk bedrag wordt ingeschreven
- Werken de partijen afdoende mee waarmee gekoppeld moet worden (een toezegging vooraf blijkt in de praktijk soms anders)
- Voortschrijdend inzicht waardoor bijstellen van het programma van Eisen en Wensen nodig is
- Aangeboden toepassingen vragen meer functionele kennis en kunde als wat in huis is
- Planningen die anders lopen door ontwikkelingen elders
etc.

8. Op de website https://basisbeveiliging.nl/#/report/227 is te zien dat er enkele risico's zijn op het gebied van websites in beheer van de gemeente. Op 10 websites wordt momenteel (15-6-2021) een hoog risico geconstateerd. Worden de bevindingen van basisbeveiliging.nl verwerkt?

Er is vanuit de gemeente Nieuwkoop geen relatie met basisveiliging.nl, maar we zullen de bevindingen verwerken.
Een eerste bevinding is dat de informatie op onderdelen verwarrend kan zijn.
Zo zijn een aantal domeinen niet meer bereikbaar, maar hier wordt bijvoorbeeld wel vermeld dat het certificaat niet betrouwbaar is. Ook zien we een diverse domeinen van Holland Rijnland met een hoog risico, die niet beheerd worden door de gemeente Nieuwkoop. Vanzelfsprekend ondernemen we hier wel actie op en nemen we contact op met de beheerders van de domeinen om hier mee aan de slag te gaan.

Alvast bedankt voor uw reactie,

Met vriendelijke groet,

D66

J. van der Pijl