

Memo Commissie Informatieveiligheid & privacy

Aanleiding

Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de dienstverlening van gemeenten. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt.

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers en organisaties ook voor gemeenten van steeds groter belang. De uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kunnen ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van gemeenten.

Gemeenten zijn schatbewaarders van vele persoonsgegevens vooral over zijn eigen inwoners. Door de toegenomen digitalisering zijn deze gegevens vanuit de hele wereld te benaderen. Dit maakt een goede beveiliging van systemen en gegevens noodzakelijk. De afgelopen jaren is een sterke toename te zien van de belangstelling van de cybercriminelen in persoonsgegevens omdat zij die gegevens kunnen gebruiken voor cybercriminaliteit. Daarbij heeft de gemeente een aantal taken erbij gekregen in het gebied van jeugdzorg en WMO die het aantal privacygevoelige gegevens hebben vergroot.

Sinds de ondertekening van de VNG-Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' hebben gemeenten werk gemaakt van informatiebeveiliging. De gemeente Woerden is bezig met de implementatie van het gemeenschappelijk normenkader van de Baseline Informatiebeveiliging Gemeenten (BIG) en hanteren dit als basis voor het gemeenschappelijk veiligheidsbeleid. Via een implementatieplan voert de gemeente een gefaseerde en gedifferentieerde implementatie van de BIG door die gebaseerd is op risicoafwegingen en financieringsmogelijkheden.

De implementatie van dit plan ligt bij de teams ICT en Informatiebeleid. De controle hiervan is belegd bij de CISO (Chief Information Security Officer)

Hiernaast kunnen ook privacy kwesties aan de orde komen, hierbij kan gedacht worden aan datalekken en klachten over schending van het privacybeginsel.

Om de Raad te faciliteren in zijn controlerende taak op het beleid en de financiën wil het college de raad graag meer inzicht geven in welke stappen wij als gemeente moeten nemen om te kunnen voldoen aan de voorschriften zoals ondertekent in de BIG. Het college stelt daarom de instelling van een halfjaarlijkse besloten commissie voor.

Doel

Het informeren van de Raad op hoofdlijnen van het van de uitvoering van het Informatieveiligheidsbeleid. Het besloten karakter van de commissie is belangrijk omdat wij de cybercriminelen geen kennis willen verlenen over de werkelijke aanvallen en genomen maatregelen.

Taken en verantwoordelijkheden

- De CISO (chief Information Security Officer) geeft elk half jaar een besloten presentatie
- Het collegelid die verantwoordelijk is voor Informatieveiligheid is hierbij aanwezig
- Bij eventuele privacykwesties (datalekken en klachten over schending van het privacybeginsel) zal de nog te benoemen Data Protection Officer (DPO) / Functionaris Gegevensbescherming (FG)¹ aanwezig zijn, het collegelid verantwoordelijk voor privacy (burgemeester) en eventueel de projectleider privacy sociaal domein
- De raadsleden moeten op hoofdlijn kennis hebben van de BIG en het interne informatieveiligheidsbeleid van de gemeente
- De raadsleden moeten kunnen inschatten welke informatie ze kunnen delen met hun mederaadsladen bij voorkeur in besloten vergaderingen

¹ In de nieuwe Europese privacyverordening (Algemene Verordening Gegevensbescherming – hierna AVG) geldt vanaf 25 mei 2016. Europese verordening (AVG).De gemeente wordt geacht om vanaf die datum hun bedrijfsvoering met de AVG in overeenstemming te brengen en krijgen daarvoor tot 25 mei 2018 de tijd. Een van de punten is het benoemen van een data protection officer