



Jaarstukken 2018



gemeente
gouda

Omschrijving	31 december 2017	31 december 2018
Bezetting in FTE	442	431
Bezetting in aantal medewerkers	496	482
Aantal gedetacheerden	8	5
Aantal medewerkers boventallig	0	5
Totaal aantal medewerkers in dienst	504	492
Deeltijdpercentage medewerkers in dienst	89%	89%

Loonkosten

Omschrijving (bedragen * € 1.000)	2017	2018
Loonkosten budget	36.696	38.083
Loonkosten realisatie	34.397	35.259

In lijn met de doelstelling blijven de loonkosten over 2018 binnen de begroting. Er is een lichte daling van het aantal FTEs in combinatie met licht hogere salarissen door de cao-stijging van 1,5% per 1 januari 2018 en het toepassen van een hogere inschaling bij instromen van nieuwe medewerkers, als gevolg van de krappe arbeidsmarkt. In 2018 is in enkele gevallen een arbeidsmarkttoelage verstrekt.

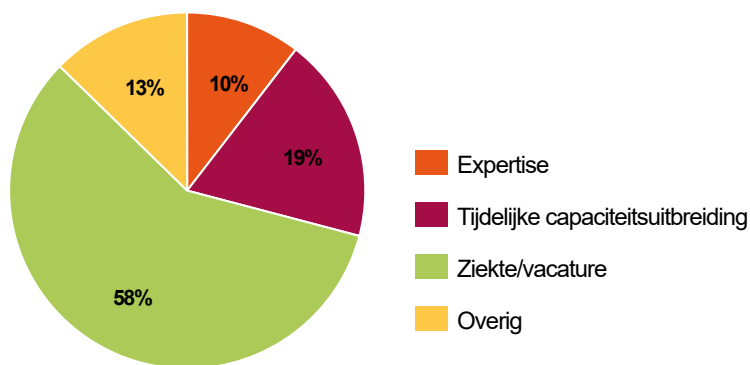
Inhuur derden

Omschrijving (bedragen * € 1.000)	2017	2018
Reguliere inhuur	7.826	7.752

In 2018 is de totale inhuur met 3% gedaald. Bij projecten waar tijdelijke dekking voor beschikbaar is, zoals subsidies en bijdragen van derden, en waar een specifieke expertise wordt gevraagd, wordt vaak gekozen voor inhuur. Daarnaast wordt uit oogpunt van continuïteit bij vertrek of ziekte van medewerkers (tijdelijke vervanging) en uitvoering van nieuwe taken soms ook gekozen voor inhuur. Dit is enkel toegestaan indien er geen eigen personeel aanwezig is en er binnen de begroting budget voor beschikbaar is.

Doordat de gemeente Gouda bij inhuur consequent gebruik maakt van een vaste 'broker', neemt het inzicht in en de grip op de inhuur toe. Hierdoor zijn er nieuwe rapportagemogelijkheden beschikbaar gekomen en heeft de organisatie nu o.a. goed inzicht in de reden van de inhuur. Dit betekent dat er vooraf een betere afweging kan worden gemaakt over de aard, vorm en omvang van de (eventuele) inhuur. Dit verklaart mede de daling van de inhuur.

Aanleiding inhuur



Aantal

4.5.4 Informatieveiligheid en Privacy

Beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en privacy zijn thema's die doorlopend aandacht nodig hebben.

4.5.4.1 Informatieveiligheid

Voor de gemeente is het uitgangspunt informatiebeveiligingsbeleid conform de Baseline Informatiebeveiliging Gemeenten (BIG). Dit kader bevat 303 beveiligingsmaatregelen onderverdeeld in technische, bouwkundige, organisatorische maatregelen om de gemeentelijke informatie te beschermen. De gemeente volgt de BIG om te voldoen aan wet- en regelgeving, voor een betrouwbare en continue dienstverlening, voor het zorgvuldig omgaan met informatie en het beheersen van risico's.

De gemeente streeft naar een optimale informatieveiligheid, maar 100% veiligheid is helaas een illusie.

Uit het onlangs verschenen Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019-2020 blijkt dat de vijf belangrijkste gesignaleerde bedreigingen voor de lokale informatievoorziening zijn:

- Informatiebeveiliging kampt met imagoprobleem;
- Inzicht in risico's is niet integraal;
- Aanvallen succesvol door ontbreken basismaatregelen;
- Te veel werk voor te weinig mensen;
- De complexiteit neemt toe.

Resultaten afgelopen periode

In de afgelopen jaren zijn de maatregelen uit de BIG opgepakt. In 2018 is vooral gestuurd op het nog beter maken van maatregelen die geheel of deels waren gerealiseerd of nog op de planning stonden voor realisatie. Dit is gedaan op basis van de resultaten ENSIA 2017 door de verbeterpunten hieruit op te volgen.

Zo is het informatiebeveiligingsbeleid geactualiseerd; is er meer geïnvesteerd in het bevorderen van kennis en bewustwording van medewerkers; is de procedure wijziging of beëindiging dienstverband herzien zodat netwerkaccounts en applicatierechten bij doorstroom worden aangepast overeenkomstig de nieuwe functie en bij uitstroom worden verwijderd; is beleid opgesteld en geïmplementeerd voor werken met informatiesystemen buiten de reguliere kantooromgeving en wordt bij nieuwe overeenkomsten gekeken of onze eisen richting leveranciers ook worden doorvertaald naar hun onderaannemers; is het functieboek aangepast waarin de lijnmanager expliciet verantwoordelijk wordt voor de integrale informatiebeveiliging van zijn of haar organisatieonderdeel en ieder jaar een in control verklaring hierover moet afgeven; is een start gemaakt met het nalopen van bestaande overeenkomsten in hoeverre leveranciers en samenwerkingsverbanden voldoende verantwoordelijk zijn gemaakt voor de privacy- en beveiligingseisen eisen vanuit AVG en BIG, en de wijze waarop hierover assurance moet worden gegeven.

Beheersmaatregelen

Om de informatiebeveiliging te monitoren wordt gebruik gemaakt van een Information Security Management Systeem dat uitgaat van de planning en control-cyclus. Verder worden alle verbeteracties geïnitieerd, bewaakt en geborgd vanuit de werkgroep Informatieveiligheid en Privacy.

Realisatie doelstelling IB-beleid (effectiviteit beheersmaatregelen en risico's)

Sinds 2017 wordt de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek gehanteerd waarmee getoetst is in hoeverre de beheersmaatregelen getroffen zijn in het kader van het IB-Beleid. Hiermee sluit de verantwoording over informatieveiligheid aan op de planning en control-cyclus van de gemeente.

Uit de zelfevaluatie 2018 blijkt dat Gouda steeds beter de goede dingen doet maar dat er enkele punten ter verbetering blijven in aanloop naar de invoering van de Baseline Informatiebeveiliging Overheid (BIO) per 1 januari 2020. De belangrijkste zijn het meer privacy by default inrichten van processen en systemen; het voor alle (kritische) processen uitvoeren van een Business Impact Analyse (BIA); het verbeteren van het incidentmanagement- en testproces; het actueel houden van en meer controleren op naleving van afgesproken werkwijzen rond informatieveiligheid en privacy met leveranciers en verbonden partijen en het verkrijgen van assurance hierop; en het blijven werken aan bewustwording informatiebeveiliging.

Naast de horizontale verantwoording is het doel van ENSIA ook om de verticale verantwoording richting de rijksoverheid, over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) te structureren.

De zelfevaluatie van BRP en PNIK (Paspoorten en Nederlandse Identiteitskaarten) bestaat sinds 2017 uit het invullen van vragenlijsten in twee instrumenten: Kwaliteitsmonitor en ENSIA.

Voor zowel BRP als PNIK is een goed resultaat behaald. De totaalscore voor de Zelfevaluatie PNIK bedraagt 98,3%. Voor de Zelfevaluatie BRP is een totaalscore van 97,2% behaald. Jaarlijks toetst RvIG inhoudelijk de kwaliteit. De gestelde normen zijn behaald en resultaten zijn via de Kwaliteitsmonitor beschikbaar gesteld.

Voor de BAG scoorden we op de onderdelen borging, volledigheid en juistheid volledig aan de gestelde eisen. Op het punt actualiteit scoren we iets lager, maar nog wel boven de gestelde norm.

Voor de BGT geldt dat op de onderdelen volledigheid en juistheid volledig aan de gestelde eisen wordt voldaan. Op het punt borging wordt iets lager gescoord maar nog wel boven de gestelde norm. Voor de BRO (basisregistratie ondergrond) is dit de eerste keer dat de ENSIA is ingevuld. Dit was op vrijwillige basis en nog niet verplicht. In september is gestart met de implementatie van de BRO door het opstellen van een impactanalyse en een plan van aanpak.

Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet

De stuurgroep ENSIA heeft besloten dat ook in het tweede jaar van ENSIA het college middels een verklaring verantwoording aflegt over de opzet en het bestaan van beheersmaatregelen en nog niet over de werking daarvan.

Het verantwoordingsjaar 2018 richt zich op de DigiD-normen en een selectie van Suwinet normen. Een onafhankelijke IT-auditor controleert de collegeverklaring en stelt een assurancerapport op waarmee verklaard wordt dat de collegeverklaring een getrouw beeld geeft.

Bovengenoemd proces is medio 2019 afgerond. Daarna wordt de collegeverklaring ENSIA inzake informatiebeveiliging SUWInet inclusief bijlage Suwinet gezamenlijk met het assurancerapport separaat van het jaarverslag aan de gemeenteraad aangeboden. DigiD valt dit jaar buiten de verantwoordingsplicht ENSIA omdat het twee nieuwe aansluitingen betreft.

Meerjarenperspectief informatieveiligheid

De komst van de AVG en het dreigingsbeeld informatiebeveiliging Nederlandse Gemeenten vragen om herijking van de uitgangspunten informatieveiligheid en actualisatie van het informatiebeveiligingsbeleid en de daarbij horende maatregelen. Deze maatregelen, implementatiemaatregelen ten behoeve van de AVG compliance en de verbeterpunten uit ENSIA zijn ingrediënten voor het verbeterplan Informatieveiligheid 2018-2019.

4.5.4.2 Privacy

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden, een direct werkende Europese wet die veel impact heeft op de verwerking van persoonsgegevens die de gemeentelijke organisatie doet. Om aan de eisen van de AVG te voldoen is het project Gouda Privacyproof opgestart. Een meerjarenproject dat in fases wordt uitgerold om de compliance van de AVG te bereiken.

In 2018 zijn 15 mogelijke datalekken geregistreerd in het daarvoor bestemde register. Daarvan zijn er 3 gemeld bij de Autoriteit Persoonsgegevens, omdat er (mogelijk) schade is en of gevolgen zijn voor de betrokkene(n).

Meerjarenperspectief privacy

In 2019 zullen de implementatiemaatregelen ten behoeve van de AVG verder worden uitgerold. De belangrijkste daarvan zijn de introductie van een Privacy Managementsysteem, het in kaart brengen van de ketenregie en het opnieuw bepalen van mogelijke risicogebieden.

4.5.5 Informatievoorziening en automatisering

Geheugen van Gouda

Het doel van het programma "Geheugen van Gouda" is de (digitale) dienstverlening te verbeteren door informatie op een betere manier te verwerken en op te slaan, zodat de informatie tevens eenvoudiger terug te vinden is. In 2018 is het technisch fundament wat zaakgericht werken mogelijk maakt aangeschaft en geïmplementeerd. Op dit fundament zijn in 2018 de eerste 5 zaakgerichte producten in gebruik genomen. Het Social Intranet is verder geïmplementeerd. Het juridisch beleidskader is geactualiseerd en waar nodig uitgebreid. Een technische oplossing voor het duurzaam toegankelijk maken en houden van ons organisatiegeheugen is in de vorm van een (pr)e-depot ingericht en gevuld met de eerste gegevensbron. Tot slot zijn de voorbereidingen voor een projectenomgeving gebaseerd op het Microsoft Office 365 platform gestart en is de basis voor een kwaliteitssysteem Informatiebeheer gerealiseerd.

Standaardisatie ICT

De organisatie heeft zich ten doel gesteld door standaardisatie het aantal applicaties waar mogelijk terug te dringen. In 2018 zijn de mogelijkheden geïnventariseerd. In het nieuwe informatieplan wordt aangegeven hoe de sturing op het aantal applicaties wordt ingericht en welke maatregelen daartoe worden genomen met o.a. aanvragen door een Wijziging Advies Commissie (WAC) te behandelen.

Met Waddinxveen en Zuidplas is een samenwerking op ICT-beheer gestart. Daarbinnen worden ook de mogelijkheden tot gemeenschappelijk gebruik van applicaties en het samen werken bij informatiekundige vraagstukken onderzocht. Vanaf de start van de overeenkomst vindt al samenwerking plaats met twee applicaties, de Microsoft - kantoorautomatisering en het licentiebeheer betreft van o.a. Microsoft, Citrix en Oracle. Het laatste is een onderdeel van de ICT-overeenkomst.

4.5.6 Aanbestedingsbeleid

In het bestuursakkoord 2018-2022 is afgesproken dat het college jaarlijks aan de hand van een steekproef rapporteert over het uitnodigen van lokale of regionale ondernemers voor meervoudig onderhandse opdrachten van de gemeente.

Uit een steekproef van 21 opdrachten die in 2018 meervoudig onderhands of enkelvoudig onderhands zijn aanbesteed, is het volgende op te merken over het betrekken van lokale en regionale ondernemers.