

### 3.4.3 Informatisering en automatisering

In 2023 is een grote inhaalslag doorgevoerd qua modernisering van de infrastructuur van de gemeente. Zowel alle servers, dataopslag, backup voorzieningen, alsook alle netwerk- en WIFI apparatuur werden geheel vervangen. Dit is gelukt zonder dat daarbij sprake was van serieuze overlast en/of uitval van services. Alle ICT dienstverlening verloopt inmiddels via deze nieuwe voorzieningen.

Ook op functioneel vlak waren er ontwikkelingen: de voorzieningen om klaar te zijn voor de omgevingswet werden ingericht en er werd mee geoefend, een aantal softwarepakketten werden aanbesteed (o.a. financiën en anonimiseringsgereedschap (met name om de wet open overheid (Woo) te faciliteren). Aan de verdere 'digitalisering van manieren van werken' werd gewerkt (vooral het terugdringen van nog bestaande papieren processen). Daarnaast werden een aantal significante marktontwikkelingen kleinschalig verkend om een eerste beeld op te bouwen wat de gemeente ermee kan (met name de opkomst van programma's met kunstmatige intelligentie zoals ChatGPT en het werken met 3D-ruimtelijke modellen).

Op programma en /projectniveau is gekeken en voorbereid hoe de gevolgen het beste kunnen worden opgevangen van het gelijktijdig actief worden van een scala aan wetten met digitale gevolgen (Wet Open Overheid, Wet modernisering elektronisch bestuurlijk verkeer, single digital gateway, eIDAS (electronic Identities), data en AI act, NIS2 (beveiliging)). De uitvoering ervan is voorzien in 2024.

### 3.4.4 Informatiebeveiliging

Jaarlijks voert de gemeente de Eenduidige Normatiek Single Information Audit (ENSIA) zelfevaluatie uit om de stand van zaken te toetsen met betrekking tot de invoering van de maatregelen van de Baseline Informatiebeveiliging Overheid (BIO). ENSIA structureert verantwoording over de basisregistraties (BRP, BAG, BGT en BRO), DigiD en SUWI. De ENSIA resultaten zijn ten opzichte van vorig jaar op hetzelfde niveau.

Een onafhankelijke IT-auditor heeft de verplichte audit over Informatiebeveiliging van DigiD en Suwinet onderzocht en goedgekeurd. Het college heeft verantwoording afgelegd over DigiD, Suwinet en de basisregistraties aan zowel de gemeenteraad als de Rijksoverheid.

In de BIO zijn gestandaardiseerde veiligheidsnormen vastgelegd voor het beschermen van informatie bij overheidsorganisaties. Het doel is aan deze normen te voldoen, dat betekent waarborgen van beschikbaarheid, integriteit, vertrouwelijkheid van informatie en de informatievoorziening binnen de overheid. Hierdoor wordt een veilige samenwerking en uitwisseling van gegevens binnen de overheid bevorderd.

We informeren en adviseren medewerkers over informatieveiligheid en geven hen handelingsperspectieven. Er loopt al enige tijd een bewustwordingsprogramma voor medewerkers.

Ook zijn er nieuwe procedures opgesteld ten behoeve van het uitvoeren van de rechten van betrokkene die vallen onder de wet Algemene verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Er zijn drie verzoeken geweest van betrokkenen die hun AVG-rechten wilden uitoefenen.

Er is een Security Incident Management en Response proces. Via dit proces worden gemelde incidenten beoordeeld en wordt actie ondernomen om eventuele schade als gevolg van een incident te voorkomen dan wel te beperken. Indien het incident grote impact kan hebben op de organisatie wordt de directie en/of de portefeuillehouder informatiebeveiliging geïnformeerd. In 2023 zijn er 19 datalekken geweest, hiervan zijn 2 datalekken als hoog risico bestempeld en om die reden ook binnen de wettelijke termijn van 72 uur gemeld bij de Autoriteit Persoonsgegevens (AP).