Strategisch beleid Informatieveiligheid en privacy ~ op hoofdlijnen, augustus 2020

De gemeente verzamelt en gebruikt veel (persoons)gegevens afkomstig van burgers, inwoners, medewerkers, andere overheidsorganisaties en (keten)partners. Deze zijn nodig om diensten en producten te leveren maar soms ook omdat het wettelijk verplicht is. De gemeente moet zorgvuldig en veilig omgaan met (persoons)gegevens en informatie. Het Strategisch beleid Informatieveiligheid en privacy beschrijft onder meer de strategische doelen, uitgangspunten en randvoorwaarden voor de beveiliging van informatie en de bescherming van persoonsgegevens. Ook gaat het in op de organisatie, taken en verantwoordelijkheden. In dit document staan de hoofdlijnen van het beleid.

Algemene uitgangspunten

- Voor zowel informatieveiligheid als privacy is een integrale aanpak vereist. Deze integrale aanpak wordt meegenomen bij de ontwikkeling (security by design en privacy by design) en de inrichting (security by default en privacy by default) van informatiesystemen, processen, diensten en producten. Maar ook bij nieuwe (incidentele en structurele) verwerkingen van persoonsgegevens.
- Informatiebeveiliging en gegevensbescherming zijn een continu verbeterproces (plan, do, check en act). De kwaliteit van de informatievoorziening en het verwerken en beschermen van persoonsgegevens wordt verankerd door periodieke controle, organisatiebrede planning en coördinatie.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om eigendommen en werkprocessen adequaat en passend te beveiligen en om de bescherming van persoonsgegevens te garanderen.

Uitgangspunten Informatieveiligheid

Vanaf 2020 is de Baseline Informatiebeveiliging Overheid (BIO) het normenkader voor de gehele overheid. Zo ook voor de gemeente. De BIO gaat over het risicogericht treffen van maatregelen om gegevens en informatie adequaat te beveiligen. De 10 bestuurlijke principes voor informatiebeveiliging van de VNG zijn een aanvulling op het normenkader van de BIO.

De belangrijkste uitgangspunten op hoofdlijnen voor informatieveiligheid zijn:
- Alle informatie en informatiesystemen zijn van belang, bepaalde informatie is van vitaal en kritiek belang.
- De interne eigenaar (afdelingshoofd in de rol van proceseigenaar) bepaalt de beveiligingsmaatregelen op basis van risicomanagement. Daar waar nodig worden extra maatregelen getroffen ten opzichte van de BIO.

Uitgangspunten Privacy

Sinds 25 mei 2018 zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG van kracht. Daarnaast zijn er andere algemene of specifieke wetten met bepalingen over het verwerken en uitwisselen van persoonsgegevens, bijvoorbeeld de Wet basisregistratie personen (BRP), de Wet politiegegevens of de Jeugdwet.

De belangrijkste uitgangspunten op hoofdlijnen voor privacy zijn:
- Het waarborgen van privacy door het beschermen van persoonsgegevens is belangrijk.
- Privacymaatregelen worden bepaald op basis van wetgeving en het privacybeleid van de gemeente, inclusief (aanvullende) privacybeleid of regels voor een specifiek domein of onderwerp.
- Als privacy moet wijken voor andere belangen, bijvoorbeeld openbare orde en veiligheid, gebeurt dit weloverwogen en bewust en op basis van een risico-inschatting.

Organisatie, taken en verantwoordelijkheden

Bestuur, directie en lijnmanagement spelen een cruciale rol bij het uitvoeren van het strategisch beleid voor informatieveiligheid en privacy. De gemeenteraad heeft een controlerende taak. Het college van B&W is bestuurlijk integraal verantwoordelijk en de directie is kaderstellend en ambtelijk verantwoordelijk. Afdelingshoofden zijn als proceseigenaren organisatorisch verantwoordelijk voor de informatiebeveiliging en gegevensbescherming binnen hun eigen organisatieonderdelen. Teamleiders zorgen voor de dagelijkse aansturing en het waar nodig aanpassen van procedures, werkprocessen en gegevensverwerkingen.

Alle medewerkers, zowel vast als tijdelijk, intern of extern, zijn verplicht het beleid en de onderliggende richtlijnen, procedures en werkinstructies na te leven. Zij moeten verantwoord, dat wil zeggen zorgvuldig en veilig, omgaan met gegevens en informatie en (vermoedelijke) beveiligingsincidenten en datalekken direct melden.

Er zijn daarnaast specifieke teams en functies die zich gemeentebreed bezighouden met informatieveiligheid en privacy. Denk aan HRM, PSA, Interne dienst, I&A, DIV, de privacy-officer (PO), en de onafhankelijke toezichthouders: de functionaris gegevensbescherming (FG) en de beveiligingsfunctionaris (CISO). Ook zijn er specifieke functies/rollen op vakgebieden zoals BRP, reisdocumenten, rijbewijzen en werk & inkomen. De gemeente heeft verder een beveiligings-adviescommissie en legt intern en extern verantwoording af over de informatieveiligheid en privacy door middel van (verplichte) audits, zelfevaluaties en interne controles en onderzoeken. Met externe partijen en andere organisaties die persoonsgegevens voor of namens de gemeente verwerken, worden schriftelijke afspraken vastgelegd over de informatiebeveiliging en gegevensbescherming.