

Doetinchem, 22 februari 2023

## Rekenkamerrapport Informatiebeveiliging en privacy

### **Te besluiten om:**

De aanbevelingen van de rekenkamer over te nemen en het college te verzoeken:

1. de positie van de CISO en de Functionaris Gegevensbescherming in een van de lijn onafhankelijke staffunctie te plaatsen en de omvang van de formatie van deze strategische functies op informatieveiligheid te verstevigen;
2. de ambitie te formuleren om het gemiddelde niveau van de medewerkers van de gemeente te verhogen;
3. de raad meer te betrekken bij het formuleren van ambities op informatieveiligheid en de raad meer te informeren over de voortgang op deze ambitie;
4. de risico's in de samenwerking op ICT te inventariseren, deze te bespreken met de partners en daarop de vernieuwde samenwerking in te richten;
5. een beleidskader op basis van de Digitale Agenda Gemeenten 2024 van de VNG op te stellen;
6. samen met de raad het gesprek aan te gaan om de vrije ruimte in het kader van ENSIA (Eenduidige Normatiek Single Information Audit) in te vullen, zodat de raad voor zijn controlerende rol zicht krijgt op opzet, bestaan en werking van de maatregelen op informatiebeveiliging en privacy;
7. de eventuele financiële consequenties van de aanbevelingen in kaart te brengen en deze voor te leggen aan de raad.

### **Context**

De rekenkamercommissie Doetinchem (hierna 'de rekenkamer') heeft een onderzoek laten uitvoeren naar het informatiebeveiligings- en privacybeleid van de gemeente. Dit onderzoek is uitgevoerd door bureau 'PRAE - advies en onderzoek' te Utrecht. Gekeken is naar het gevoerde beleid, de organisatie, de techniek en het menselijk handelen.

### **Het onderzoek**

De centrale onderzoeksvraag was als volgt: "Welke kwetsbaarheden kent de beveiliging van de vertrouwelijkheid van de informatie van de gemeente en op welke wijze gaat de gemeente om met de privacygevoelige gegevens en informatie waarover zij beschikt?"

Uit het onderzoek van de rekenkamer blijkt dat het over het algemeen op orde is, maar dat betekent niet dat de gemeente tevreden achterover kan leunen; er is werk aan de winkel.

### **Conclusies rekenkamer**

De rekenkamer concludeert dat de gemeente Doetinchem nog een ontwikkeling heeft door te maken om 'in control' te komen op informatieveiligheid. De gemeente onderneemt de stappen om te voldoen aan het beleid op informatiebeveiliging en privacy, samen het informatieveiligheidsbeleid. Verder concludeert de rekenkamer dat:

1. het informatiebeveiligings- en privacybeleid op orde zijn;
2. de technische kant op orde is, maar beter gemonitord moet worden;
3. het volwassenheidsniveau van de organisatie ontwikkeling behoeft;
4. de essentiële functies op deze terreinen kwetsbaar zijn ingevuld en onvoldoende onafhankelijk gepositioneerd zijn;|

Doetinchem, 22 februari 2023

5. de bewustwording bij medewerkers groeiend is, maar een groot aandachtspunt is en blijft.
6. de regionale samenwerking met Doetinchem als gastheer risico's kent die onvoldoende zijn afgedekt in de dienstverleningsovereenkomst;
7. de gemeenteraad te summier wordt geïnformeerd;
8. datagestuurd werken en koppeling van gegevens in de kinderschoenen staan. Ook is er (nog) geen beleid geformuleerd.

### **Aanbevelingen**

Bovenstaande conclusies leiden tot de volgende aanbevelingen aan raad en college:

1. Verminder de kwetsbaarheid van de formatie op informatieveiligheid en privacy en positioneer deze functionarissen buiten 'de lijn'.
2. Houd de technische systemen voor informatieveiligheid op orde.
3. Zet sterk in op het bevorderen van het bewustzijn van medewerkers.
4. Versterk de governance en afspraken op de regionale samenwerking op ICT-gebied.
5. Informeer de raad meer en inhoudelijke over dit onderwerp en bepaal het ambitieniveau.
6. Stel een beleidskader op voor de transformatie van de digitale dienstverlening.

### **Bestuurlijke reactie**

De laatste jaren heeft de beeldvormende raad verzocht om een reflectie van het college op aanbevelingen van de rekenkamer in onderzoeksrapporten, alvorens het rekenkamer-rapport in de menings- en besluitvormende raad te bespreken.

Het presidium heeft daarom aan de griffie verzocht om, in samenspraak met de rekenkamer, de Verordening op de rekenkamer en het onderzoeksprotocol op dit punt aan te passen.

Vooruitlopend op deze wijziging heeft de rekenkamer het college om een bestuurlijke reactie op dit onderzoek gevraagd.

In de bestuurlijke reactie geeft het college aan de aanbevelingen voor een deel te herkennen. Deze neemt het college dan ook over. Een deel van de aanbevelingen is volgens het college niet compleet en/of vraagt nuancering.

Wat betreft de algemene conclusie geeft het college aan dat deze erg algemeen gesteld is. Het college geeft aan dat de gemeente in ontwikkeling is. Het terrein van informatiebeveiliging en privacy is groeiend en complex. Daardoor is het wellicht pretentius om te kunnen stellen dat de gemeente volledig "in control" is. Er zijn en worden veel inspanningen gedaan aan het beschermen, beheren en beheersen van alle informatie van de gemeente Doetinchem.

Als het gaat over de meer wettelijke, organisatorische en technisch infrastructurele informatieveiligheidsmaatregelen meent het college dat Doetinchem in vergelijking met andere gemeenten relatief gezien 'goed in control' is. Dit geldt zowel als gemeente Doetinchem, maar ook gezamenlijk binnen de ICT-samenwerking.

Wat betreft de eerste aanbeveling ('versterk de positie van de strategische functionarissen op informatiebeveiliging en privacy en plaats deze in een staffunctie') geeft het college aan op dit moment geen staffuncties te kennen die los staan van teams, ook de FG en de CISO. Zij hebben echter hun eigen onafhankelijke taken, verantwoordelijkheden en escalatiemogelijkheden naar de gemeentesecretaris en de bestuursorganen. Wat betreft de positionering vindt het college dat deze onafhankelijkheid en escalatielijn belangrijke pijlers zijn.

In de begroting 2023 is opgenomen dat de budgetten voor versterking van de ICT-organisatie tegen specifieke ICT-dreigingen worden geïntensiveerd. Vanaf 2023 is dit structureel.

Ook wordt € 100.000 extra ingezet voor de taken die voortvloeien uit de Wet politiegegevens (Wpg).

Doetinchem, 22 februari 2023

Door een toename van taken zijn de huidige uren van de Functionaris Gegevensbescherming en Privacy Coördinator niet meer toereikend. Met de extra middelen wil het college formatie en de werkprocessen passend maken. Ook zet het college in op meer bewustwording en kennis bij alle collega's in onze organisatie.

Het college onderschrijft het belang van aanbeveling twee ('formuleer de ambitie om het gemiddelde niveau van de medewerkers van de gemeente te verhogen') en gaat een ambitie formuleren die wordt opgenomen in het informatiebeveiligingsbeleid.

De aanbeveling van de rekenkamer om de raad meer te betrekken bij het formuleren van ambities op informatieveiligheid en de raad meer te informeren op de voortgang van deze ambities, worden door de FG en CISO besproken met de portefeuillehouder.

Het college geeft aan dat aanbeveling vier ('Inventariseer de risico's in de samenwerking op ICT, bespreek deze met de partners en richt daarop de vernieuwde samenwerking in') juist is en in deze vorm feitelijk wordt uitgevoerd. Het college ziet het als aansporing om dit voort te zetten.

Wat betreft aanbeveling vijf om een beleidskader op te stellen op basis van de Digitale Agenda Gemeenten 2024 van de VNG geeft het college aan dit beleidskader in het informatieveiligheidsbeleid mee te nemen.

Over de opmerking van de rekenkamer dat de ICT-samenwerking, waarvan Doetinchem gastheer is, risico's kent die niet afdoende zijn afgedekt in de dienstverleningsovereenkomst geeft het college het volgende aan.

Binnen de ICT-samenwerking werkt Doetinchem goed samen met vier andere gemeenten en een aantal andere overheden. De afspraken over de omvang en kwaliteit van de dienstverlening worden regelmatig herijkt en de dienstverleningsovereenkomst wordt dan ook voortdurend verbeterd en actueel gehouden.

### **Argumenten**

Tijdens de behandeling van dit raadsvoorstel kunt u uw mening geven over de aanbevelingen uit het rapport en de reactie van het college. U kunt via amendementen en moties de beslispunten wijzigen.

In de bestuurlijke reactie geeft het college aan op welke wijze het invulling geeft aan de aanbevelingen van de rekenkamer.

### **Financiën**

De uitvoering van de aanbevelingen heeft waarschijnlijk financiële consequenties. Het college wordt verzocht deze in kaart te brengen en voor te leggen aan de raad.

### **Bijlagen**

1. Bestuurlijke nota rekenkamerrapport Informatiebeveiliging en privacy
2. Samenvatting onderzoek digitale veiligheid en privacy
3. Nota van bevindingen Informatiebeveiliging en privacy
4. Bestuurlijke reactie rekenkameronderzoek informatieveiligheid
5. Nawoord rekenkamercommissie Doetinchem

De griffier,

drs. B.P.M. Janssens

De voorzitter,

mr. M. Boumans MBA MPM

De raad van de gemeente Doetinchem;

gezien het voorstel van burgemeester en wethouders over Rekenkamerrapport Informatieveiligheid en privacy;

gelet op artikel 108, lid 1, juncto artikel 147, lid 2 van de Gemeentewet;

b e s l u i t :

de aanbevelingen van de rekenkamer over te nemen en het college te verzoeken:

1. de positie van de CISO en de Functionaris Gegevensbescherming in een van de lijn onafhankelijke staffunctie te plaatsen en de omvang van de formatie van deze strategische functies op informatieveiligheid te verstevigen;
2. de ambitie te formuleren om het gemiddelde niveau van de medewerkers van de gemeente te verhogen;
3. de raad meer te betrekken bij het formuleren van ambities op informatieveiligheid en de raad meer te informeren over de voortgang op deze ambitie;
4. de risico's in de samenwerking op ICT te inventariseren, deze te bespreken met de partners en daarop de vernieuwde samenwerking in te richten;
5. een beleidskader op basis van de Digitale Agenda Gemeenten 2024 van de VNG op te stellen;
6. samen met de raad het gesprek aan te gaan om de vrije ruimte in het kader van ENSIA (Eenduidige Normatiek Single Information Audit) in te vullen, zodat de raad voor zijn controlerende rol zicht krijgt op opzet, bestaan en werking van de maatregelen op informatiebeveiliging en privacy;
7. de eventuele financiële consequenties van de aanbevelingen in kaart te brengen en deze voor te leggen aan de raad.

Aldus besloten in zijn vergadering van 2 maart 2023,

, griffier

, voorzitter