Programmaplan informatietransitie 2026, Plan van aanpak Weerbaarheid en Informatieveiligheid 2025-2027 en zesde rapportage Autoriteit Persoonsgegevens

Vz, Vandaag spreken wij over een aantal stukken met betrekking tot informatieveiligheid. Stukken die raken aan de kern van onze verantwoordelijkheid als overheid: het zorgvuldig omgaan met gegevens van inwoners, ondernemers en medewerkers. Dank voor de informatie die we tijdens de technische sessie van 4 maart hebben ontvangen.

Digitale veiligheid is geen technische bijzaak, maar een morele opdracht. Wie gegevens verzamelt, draagt verantwoordelijkheid. Zeker wanneer het gaat om kwetsbare data zoals persoonsgegevens en financiële informatie, moeten wij als overheid betrouwbaar en zorgvuldig zijn.

Er worden de nodige cybersecurity risico's geschetst omdat de huidige informatiebasis van de provincie niet is ingericht voor de gewenste manier van samenwerken. De oplossing die aangedragen wordt, is het vernieuwen van de samenwerkingsomgeving naar de structuur van Microsoft 365.

Vz, we hebben het in november vorig jaar gehad over de ongewenste afhankelijkheid van o.a. Microsoft. GS schrijft dat er momenteel geen volwaardig Europees alternatief voorhanden is. Goed dat GS actief blijft zoeken naar een serieus Europees alternatief.

Voorzitter, het is goed dat er over het datalek voortgang wordt gerapporteerd en dat de aanbevelingen van de Autoriteit Persoonsgegevens serieus zijn opgepakt. Tegelijkertijd constateert mijn fractie dat het traject langdurig en complex is. Dat begrijpen wij. Maar juist daarom is blijvende scherpte nodig. In dit kader is het opvallend dat ondanks de grote aandacht voor dit onderwerp het niet gelukt is om voor het verlopen van de deadline van 31 december 2025 het verwerkingsregister compleet te hebben. We lezen dat dit komt door problemen in de aansturing. Goed dat er is ingegrepen, maar kennelijk te laat om te voorkomen dat de door de AP gestelde deadline zou verstrijken.

- ➔ Het betreft hier voornamelijk een verantwoordelijkheid van de directie, maar hoe heeft GS geacteerd? Hoe heeft de gedeputeerde zijn bestuurlijke verantwoordelijkheid ingevuld?

Wij lezen over het verhogen van de ‘privacyvolwassenheid’. Dat is een belangrijk streven. Uit de technische sessie van vorige week vernamen we dat in Q2 een voorstel wordt opgesteld over o.a. monitoring. We kijken uit naar het voorstel.

In het Plan van Aanpak Weerbaarheid en Informatieveiligheid zien wij stevige ambities op het gebied van technische maatregelen, bewustwording en governance. Dat is positief.

➔ Is geborgd dat er voldoende formatie is om ambities waar te maken?

Voorzitter, vertrouwen komt te voet en gaat te paard. Een datalek schaadt niet alleen betrokkenen, maar ook het vertrouwen in de overheid als geheel. Transparantie is daarom cruciaal. Digitalisering biedt kansen voor efficiëntere dienstverlening en betere beleidsinformatie. Maar met ruim 300 softwaretoepassingen is het aanvalsoppervlak best groot.

De positie van GS is helder in de stukken. De positie van PS als controlerend orgaan niet. Sterker nog: PS wordt niet eens genoemd! Hoe wordt de controlerende rol van de Provinciale Staten van Zuid-Holland versterkt? In de technische sessie hoorden we dat we ook een e-learning kunnen volgen. Dat is mooi, wat ons betreft niet voldoende.

➔ Het CDA wenst een jaarlijkse rapportage over de staat van informatieveiligheid en privacy, inclusief resterende risico's. Kan GS dat toezeggen?

Voorzitter, digitale veiligheid is geen project met een einddatum. Het is een continu proces van verbeteren, leren en bijsturen. Als overheid moeten wij het goede voorbeeld geven: zorgvuldig, transparant en dienstbaar.

Het CDA zal de uitvoering van deze plannen kritisch maar constructief blijven volgen. Niet uit wantrouwen, maar uit verantwoordelijkheid – voor de bescherming van kwetsbare data en voor het vertrouwen van de inwoners die wij dienen. Zo geven we invulling aan de controlerende taak die wij als hoogste politieke orgaan van de Provincie hebben.