Beantwoording Technische en beeldvormende vragen voor de commissie Bestuur & Economie van woensdag 26 februari 2025 agendapunt 9.

Vragen van : D66
Aan wethouder : J.E.M.G. Göbbels
Over : Strategisch gegevensbescherming- en informatiebeveiligingsbeleid

1. Wat zijn de belangrijkste nieuwe maatregelen in het gegevensbescherming- en informatiebeveiligingsbeleid 2025-2029 vergeleken met het eerdere beleid?

2. Hoe groot is de formatie in Hilversum voor de FG (functionaris voor de gegevensbescherming) en hoe verhoudt dit zich tot vergelijkbare gemeenten?

3. Hoe worden medewerkers getraind en bewust gemaakt van hun rol in gegevensbescherming en informatiebeveiliging?

4. Zouden medewerkers niet ook onderdeel moeten uitmaken van de 'first line of defence', naast lijnmanagers, aangezien medewerkers direct met de data handelen?

5. Wat zijn de grootste externe dreigingen m.b.t. informatie- en gegevensbeveiliging en wat doet de gemeente hiertegen?

6. In hoeverre maakt de gemeente gebruik van Whatsapp en andere systemen die meta data verzamelen? En zijn er plannen om over te stappen naar/ de optie te bieden van veiligere alternatieven (zoals Signal)?

Groeten,

Laurens Verburg

Antwoord -penvoerder is Theo Buijtenweg tel: 0622261830

D66 heeft technische vragen gesteld over agendapunt 9, Strategisch gegevensbescherming- en informatiebeveiligingsbeleid, van de commissie Bestuur & Economie van 26 februari 2025.

De vragen en de antwoorden daarop vindt u hieronder

Wat zijn de belangrijkste nieuwe maatregelen in het gegevensbescherming- en informatiebeveiligingsbeleid 2025-2029 vergeleken met het eerdere beleid?

Er is gekozen voor de term "gegevensbescherming" in plaats van privacy. Gegevensbescherming ziet op meer dan alleen het grondrecht op privacy. Dit doet meer recht aan de uitgangspunten van de Algemene Verordening Gegevensbescherming (AVG).

Daarnaast is er een koppeling gemaakt met het informatiebeveiligingsbeleid en is dit samengevoegd in één beleidsdocument. Ook zijn in het beleid de kaders voor omgang met gegevens die vallen onder de Wet politiegegevens opgenomen.

Hoe groot is de formatie in Hilversum voor de FG (functionaris voor de gegevensbescherming) en hoe verhoudt dit zich tot vergelijkbare gemeenten?

Hilversum heeft geen FG in dienst maar heeft voor de invulling van de FG taken een dienstverleningsovereenkomst met Privacy Management Partners (PMP). Daarnaast is er binnen de organisatie een Privacy en informatiebeveiligingsteam (PIT). Het PIT bestaat uit professionals op het gebied van de AVG, processen en informatiebeveiliging en is belast met de ondersteuning en advisering van de organisatie. De FG heeft hierdoor een onafhankelijke positie in de uitvoering van zijn taken. Binnen de dienstverleningsovereenkomst zijn tussen directie en FG afspraken vastgelegd over de (basis)uren inzet. Binnen de begroting is hiervoor budget gereserveerd.

Hoe worden medewerkers getraind en bewust gemaakt van hun rol in gegevensbescherming en informatiebeveiliging?

Via de Hilversum academie wordt aan alle medewerkers een verplicht te volgen traject van e-learning aangeboden. Nieuwe medewerkers dienen deze trainingen, inclusief bijbehorende toetsen, binnen drie maanden na indiensttreding te hebben afgerond. Ook wordt door het PIT voorlichting gegeven in MT's en werkoverleggen en worden werk-instructies en handreikingen geschreven.

Zouden medewerkers niet ook onderdeel moeten uitmaken van de 'first line of defence', naast lijnmanagers, aangezien medewerkers direct met de data handelen?
Dat klopt, zij zijn ook de belangrijkste schakel in de gegevensbescherming en vormen daarmee de "first line of defence". We hebben er echter voor gekozen om hier expliciet de rol van de teammanager als proceseigenaar van de uitvoering te vermelden. Gegevensbescherming en informatiebeveiliging binnen de (bedrijfs)processen (procesbeschrijvingen en instructies) zijn geborgd.

Wat zijn de grootste externe dreigingen m.b.t. informatie- en gegevensbeveiliging en wat doet de gemeente hiertegen?

De bedreigingen voor de gemeente Hilversum zijn niet afwijkend van de bedreigingen voor andere gemeenten. De informatiebeveiligingsdienst (IBD, een onderdeel van de VNG) geeft elke 2 jaar een actueel dreigingsbeeld uit. In dat stuk staan ook diverse risicobeperkende maatregelen die getroffen kunnen worden om de dreigingen te mitigeren.
De laatste versie van het dreigingsbeeld staat op de site van de IBD: Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023 → 2024.

Jaarlijks verantwoord de gemeente Hilversum zich intern en extern via de ENSIA systematiek over o.a. de informatiebeveiliging.

In hoeverre maakt de gemeente gebruik van WhatsApp en andere systemen die meta data verzamelen? En zijn er plannen om over te stappen naar/ de optie te bieden van veiligere alternatieven (zoals Signal)?

Op dit moment wordt binnen de dienstverlening door het klantencontactcentrum gebruik gemaakt van een gemeentelijke zakelijke Whatsapp account. Hiermee kunnen inwoners op een laagdrempelige wijze korte vragen of meldingen doen. Wij wijzen inwoners erop dat dit kanaal niet beschikbaar is voor het doen van aanvragen of het versturen van (persoons)gegevens. Het gebruik van sociale media is een breed gebruik in de samenleving en allang niet meer beperkt tot Whatsapp, Signal of facebook Messenger.

Naast het gemak van het gebruik zijn er steeds vaker vragen over de veiligheid en het verzamelen van gebruikersdata (als verdienmodel van "gratis" diensten) en de morele kant van de intenties van grote techbedrijven. Dit vraagt om een heldere analyse over de vraag hoe we als gemeente hiermee willen omgaan.

Momenteel wordt vanuit informatiemanagement in samenwerking met communicatie onderzocht hoe we als gemeente hiermee om moeten gaan. De keuze en richtlijnen worden dit jaar in het college worden besproken.