GEMEENTE WAALRE

Aan de leden van de gemeenteraad van Waalre

Uw brief van	Uw kenmerk	Afdeling/Ambtenaar
		Marina Boer
Onderwerp	**Ons kenmerk**	**Datum**
Verantwoording ENSIA/ jaarverslag 2025 informatiebeveiliging en privacy	1111682	VERZONDEN 14 APR. 2026

Geachte leden van de raad,

Via deze raadsinformatiebrief informeert het college u over de wijze waarop de gemeente Waalre in 2025 uitvoering heeft gegeven aan informatiebeveiliging en privacy. Ook geeft het college een korte vooruitblik op de ontwikkelingen op het gebied van informatiebeveiliging en privacy en de daarbij behorende uitdagingen.

Digitale samenleving
Digitalisering is niet meer alleen een onderwerp van de ICT-afdeling. Het verschuift juist naar de kern van de samenleving en het functioneren van de overheid. De samenleving is digitaal in transitie en verandert snel. Zo is het vanzelfsprekend en bijzonder belangrijk om aandacht te besteden aan duidelijke taal en digitale toegankelijkheid. Deze is niet slechts beperkt tot digitale ontsluiting alleen. Taalgebruik en duidelijke verwijzingen zijn een belangrijk onderdeel van digitale ontsluiting Tegelijkertijd groeit het belang van digitale weerbaarheid, omdat cyberincidenten en -aanvallen steeds vaker voorkomen. Dit biedt ons de kans om onze digitale veiligheid verder te versterken. De gemeenten krijgen – en ook de samenleving – krijgen te maken krijgen met nieuwe vraagstukken. Onder andere op het gebied van de bescherming van een betrouwbare overheid in de informatiesamenleving, privacy en digitale veiligheid.

Om de digitale samenleving in goede banen te leiden, is wet- en regelgeving ontwikkeld: onder andere de Algemene Verordening Gegevensbescherming (AVG), Wet politiegegevens (Wpg) en de Baseline Informatiebeveiliging Overheid (BIO). Deze wet- en regelgeving waarborgt het grondwettelijk recht op privacy en zorgt voor spelregels op het gebied van informatiebeveiliging en persoonsgegevens. Daarbij beschikt de gemeente over veel gegevens, die vaak ook gevoelig van aard zijn. De burger moet erop kunnen vertrouwen dat de overheid zorgvuldig en transparant met deze gegevens omgaat. Persoonsgegevens worden verwerkt volgens specifieke wetgeving; de gemeente mag bijvoorbeeld niet meer

persoonsgegevens verwerken dan noodzakelijk is. Dit houdt onder andere in dat de gemeente haar gegevens goed moet beveiligen en transparant moet zijn over het gebruik hiervan.

Terugblik op 2025
In 2025 heeft de gemeente Waalre belangrijke stappen gezet om haar informatiebeveiliging en privacy te versterken. Er is een nieuwe meting verricht die inzicht geeft in het normenkader van de BIO en de stand van zaken van de gemeente op het moment van de meting. Deze gap-analyse laat zien dat er grote vooruitgang is geboekt: de score steeg van 81% in 2024 naar 90% in 2025. Deze vooruitgang is onder andere het gevolg van de inrichting van de moderne werkplekken. De moderne werkplek biedt een veilige en flexibele omgeving waarbij een aantal kernfactoren beschermen tegen interne en externe dreigingen. Een positieve ontwikkeling die laat zien dat onze kritische processen steeds beter worden ingericht en we meer en meer in control komen.

De samenwerking met een externe partner heeft geleid tot een flinke verbetering in onze crisisvoorbereiding bij cyberincidenten. De Cybercrisis Oefenkalender met daarin opgenomen een cybercrisistraining en een simulatieoefening, biedt vertrouwen om goed beslagen ten ijs te komen voor het geval de organisatie te maken krijgt met een cybercrisisincident.

Daarnaast is verder gewerkt aan het versterken van privacy en het naleven van de AVG en Wpg. Het verwerkingsregister en het instrument om bij een (nieuw) proces, beleid of systeem de privacyrisico's van een gegevensverwerking in kaart te brengen (de DPIA-procedure) zijn doorontwikkeld, al kost het wegwerken van achterstanden nog tijd. Bewustwording onder medewerkers blijft een doorlopend speerpunt, zodat persoonsgegevens veilig worden verwerkt en incidenten tijdig worden gemeld.

Kortom: Waalre is in 2025 duidelijk gegroeid in volwassenheid op het gebied van informatiebeveiliging en privacy. We blijven gericht werken aan verdere verbetering.

Resultaat ENSIA 2025
De informatiebeveiliging van de gemeente wordt jaarlijks getoetst met de Eenduidige Normatiek Single Information Audit (ENSIA). Deze ENSIA is verplicht en heeft tot doel het verantwoordingsproces over informatiebeveiliging bij overheidsorganisaties verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de eigen planning & control-cyclus:

Een externe auditor toetst:
- Het gebruik van de gemeente van Digitale persoonsidentificatie (DigiD);
- Het gebruik door de gemeente van de Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet, het inzien van inkomensgegevens van burgers).

Voor het jaar 2025 heeft de externe IT-auditor geoordeeld dat de collegeverklaring inclusief de bijlagen DigiD voor Care, e-Diensten en Suwinet, in alle van materieel belang zijnde aspecten, juist is. Waalre voldoet hiermee voor deze onderdelen aan de verplichtingen.

In 2025 zijn er drie informatiebeveiligingsincidenten gemeld. Eén melding ging over een technische verbinding van een privé-device, één melding betrof een verdachte authenticatie van een disabled account en één melding had te maken met een mogelijke kritieke bug in de mailfunctionaliteit van een externe samenwerkingspartner. Alle meldingen hadden geen directe consequenties voor de organisatie.

Verzoeken van betrokkenen
In 2025 zijn er drie verzoeken in het kader van de AVG binnengekomen. Twee daarvan waren feitelijk verzoeken voor de basisregistratie personen (BRP) en zijn door team Burgerzaken verder afgehandeld. De procedure voor het derde verzoek loopt nog. Na een bezwaarprocedure is de aanvrager nu in beroep gegaan.

Verzoeken verstrekking persoonsgegevens aan derden
In 2025 zijn er 117 verzoeken ontvangen van derden tot verstrekking van persoonsgegevens uit de basisregistratie personen (BRP). Hierbij kan gedacht worden aan verzoeken van bijvoorbeeld een advocaat of notaris. Team Burgerzaken geeft desgevraagd aan dat er geen bijzonderheden zijn geweest bij de afhandeling van deze verzoeken.

Vooruitblik op 2026
De gemeente krijgt te maken met de nieuwe Europese Cybersecuritywet, de NIS2. De NIS2 wordt omgezet in de nationale Cyberbeveiligingswet. Deze wet gaat naar verwachting de eerste helft van 2026 in en wordt juridisch verankert in de BIO2. De BIO2 wordt het verplichte kader om te voldoen aan de zorgplicht uit de Europese NIS2-richtlijn. Dit maakt organisatiebeveiliging niet langer vrijblijvend, maar wettelijk verplicht voor overheidsorganisatie.

In de BIO2 zijn enkele belangrijke veranderingen doorgevoerd:
- De BIO2 introduceert striktere eisen op het gebied van 'basishygiëne' (o.a. MFA, patchmanagement) en 'ketenhygiëne' (beheersing van risico's bij leveranciers.
- Het inrichten van een Information Security Management System (ISMS) volgens de ISO 27001–norm wordt verplicht gesteld.
- De BIO2 is in lijn gebracht met de NIS2-richtlijn, specifiek artikel 21 over cyberbeveiligingsmaatregelen.
- Overheidsbreed worden standaarden voor internetveiligheid versneld ingevoerd, versterkt door het "Besluit beveiligde verbinding met overheidswebsites en -webapplicaties".

Kortom, de overheid verschuift naar een meer risicogerichte en verplichte aanpak van informatiebeveiliging (BIO2 en NIS2) om de digitale weerbaarheid te versterken.

Daarnaast gaan we in 2026 inzetten op:
1) ENSIA-audit over het jaar 2026. De jaarlijkse ENSIA-rapportage is hét verantwoordingsinstrument over de staat van informatiebeveiliging. Onder de nieuwe Cyberbeveiligingswet wordt de ENSIA-rapportage zelfs nog belangrijker, omdat de gemeente daarmee aan de raad, de stelselhouders en de toezichthouders binnen de rijksoverheid kan aantonen dat zij 'in control' is en dus of ze voldoet aan de zorgplicht.
2) De procedures Data Protection Impact Assessment (DPIA). De achterstallige DPIA's worden opnieuw opgesteld en waar nodig worden maatregelen getroffen.

3) De concrete voorbereiding op de nieuwe Cyberbeveiligingswet. Dit gaan we doen door te blijven werken volgens de BIO-standaarden, waarin de eisen van de NIS2 zijn opgenomen. Maar ook door gestructureerd te blijven werken volgens het Informatie Security Management System (ISMS). Hiermee wordt de status van informatiebeveiliging blijvend gemonitord en is continue verbetering mogelijk. De Cyberbeveiligingswet stelt training over informatiebeveiliging voor bestuurders verplicht. Een dergelijke training helpt de bestuurder om de juiste vragen te stellen aan de organisatie om de voorgestelde beveiligingsmaatregelen af te kunnen wegen in relatie tot het risico voor de continuïteit van de gemeentelijke dienstverlening.

Hoogachtend,

BURGEMEESTER EN WETHOUDERS VAN WAALRE,

De secretaris a.i.

mr. S.R.M. Cammemeijer

De burgemeester,

M.F. Oosterveer