

Aan de leden van de gemeenteraad van Waalre

Uw brief van

Uw kenmerk

Afdeling/Ambtenaar

Marina Boer
N. de Ridder

Onderwerp

Verantwoording ENSIA/
jaarverslag 2024
informatiebeveiliging en privacy

Ons kenmerk

924715

Datum

VERZONDEN 22 APR. 2025

Geachte leden van de raad,

Via deze raadsinformatiebrief informeert het college u over de wijze waarop de gemeente Waalre in 2024 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 Agenda: regie op één digitale samenleving

In de Digitale Agenda Gemeenten wordt uitgebreid ingegaan op het feit dat digitalisering niet meer alleen een onderwerp van de ICT-afdeling is. 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.

Maar ook cyberincidenten en -aanvallen doen zich steeds vaker voor, onze digitale veiligheid staat op het spel. Dit zorgt ervoor dat gemeenten – en ook de samenleving – 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. Gemeenten laten met deze agenda zien hoe zij de komende jaren de kansen benutten die digitalisering biedt, voor grote maatschappelijke opgaven en om de dienstverlening nog beter aan te laten sluiten bij de eisen en verwachtingen van de samenleving.

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 om gaat. 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 2024

In 2024 is er weer een flink aantal stappen gemaakt. Er is een uitgebreide risico-analyse, de zogeheten GAP-analyse, uitgevoerd. Deze meting geeft inzicht in het normenkader van de BIO en de stand van zaken van de gemeente Waalre op het moment van de meting. De meting is het vertrekpunt van de ambitie van Waalre in relatie tot de BIO-domeinen en wordt jaarlijks opnieuw uitgevoerd. Uit de meting is gebleken dat de organisatie in 2024 ruim hoger scoort (81%) dan het jaar ervoor (70%). Een positieve ontwikkeling die laat zien dat onze kritische processen steeds beter worden ingericht en we meer en meer in control komen voor wat betreft de uitvoering van de BIO.

Ook heeft er een flinke inhaalslag plaatsgevonden op het gebied van de Data Protection Impact Assessments (DPIA's): er is een nieuwe procedure vastgesteld en er is gestart met een bewustwordingstraject op het gebied van de DPIA's.

Blijvende aandacht is er nodig voor bewustwording. De onbekendheid en onwetendheid van de medewerkers zijn en blijven het grootste risico voor dagelijkse beveiligingsrisico's en (potentiële) datalekken. Ook in 2024 is hier weer veel aandacht aan besteed. Er is een nieuw bewustwordingsbeleid vastgesteld. Dit beleid is uitgewerkt in een plan van aanpak voor 2024 en 2025 en er hebben diverse gerichte bewustwordingsacties plaatsgevonden. Door alle inspanning is duidelijk te merken dat de organisatie groeit in het bewustwordingsproces. Een positieve ontwikkeling!

Resultaat ENSIA 2024

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 2024 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. Voor wat betreft de bijlage DigiD-Zaaksysteem scoren de normen identiteit- en toegangsbeheer en wijzigingsbeheer niet voldoende. Voor deze twee normen is een verbeterplan gemaakt en opgeleverd.

Daarnaast zijn er zelfevaluaties uitgevoerd over diverse basisregistraties. Dit gebeurt door het invullen van digitale vragenlijsten. Op al deze onderdelen scoren we over het geheel gezien (ruim) voldoende.

Incidentmeldingen informatiebeveiliging

In 2024 zijn er drie informatiebeveiligingsincidenten gemeld. Twee van deze meldingen kwamen van een externe samenwerkingspartner. De meldingen hadden betrekking op een cyberaanval met ransomware en een gerichte phishingmail-actie. De incidenten hadden geen directe consequenties voor Waalre.

Het derde incident betrof een malwarebesmetting op een laptop van één van onze medewerkers. Het ging hierbij om een informatie-stealer, gericht op het verzamelen van gevoelige gegevens. Na ontdekking is direct het account en de laptop van de betreffende medewerker uitgeschakeld. Uit het onderzoek is gebleken dat de informatie-stealer geen schade heeft aangericht aan de organisatie.

Verzoeken van betrokkenen

In 2024 zijn er vijf 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. Bij twee verzoeken is om een verduidelijking gevraagd. Hierop is geen reactie meer ontvangen. Deze verzoeken zijn daarom buiten behandeling gesteld. Eén verzoek is volledig afgehandeld, hierbij heeft de verzoeker alle gevraagde gegevens en informatie ontvangen.

Verzoeken verstrekking persoonsgegevens aan derden

In 2024 zijn er 110 verzoeken ontvangen van derden tot verstrekking van persoonsgegevens uit de BRP. Hierbij kan gedacht worden aan verzoeken van bijvoorbeeld een advocaat of notaris. Bij de afhandeling van deze verzoeken zijn geen bijzonderheden geweest.

Vooruitblik op 2025

In 2025 zal er aandacht zijn voor een veilige en open organisatie. Dit is essentieel. Medewerkers moeten gebruik kunnen maken van veilige applicaties. Ook moeten medewerkers zich vrij voelen om fouten te melden. Dit zorgt ervoor dat fouten en risicovolle processen naar buiten komen en kunnen worden aangepast. Voor het bestrijden van cybercriminaliteit zal de samenwerking worden gezocht met integrale veiligheid. Er wordt geoefend in het omgaan met een cyberaanval of-crisis met zowel het bestuur als de medewerkers.

Daarnaast gaan we in 2025 inzetten op:

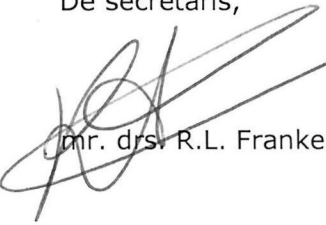
- 1) de verbetermaatregelen die zijn voortgekomen uit de ENSIA-audit 2024. Met name de normen die betrekking hebben op het identiteit- en toegangsbeheer en wijzigingsbeheer voor de bijlage DigiD-Zaaksysteem.
- 2) ENSIA-audit over het jaar 2025. De jaarlijkse ENSIA-rapportage is hét verantwoordingsinstrument 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.
- 3) De procedure voor het aangaan van verwerkingsovereenkomsten geactualiseerd en wordt de verkenning naar nieuwe software voor het verwerkingsregister voortgezet. Daar waar nodig worden verwerkingsovereenkomsten met externe partijen afgesloten.

- 4) 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,


Mr. drs. R.L. Franken

De burgemeester,


M.F. Oosterveer


b.v.