Strategisch Informatiebeveiligings- en Privacybeleid Gemeente Waalre

2023-2027

GEMEENTE WAALRE

Februari 2023
CISO en FG

Inhoudsopgave

1. Inleiding

Deze beleidsnota beschrijft het Strategisch Informatiebeveiligings- en Privacybeleid voor de jaren 2023 tot en met 2027 en vervangt het in 2019 vastgestelde 'Beleidskader Informatieveiligheid- en privacy [2019-2022]'. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Informatiebeveiligings- en Privacybeleid van 2023-2027' zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te versterken en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG. Voor privacy geldt als basis de wetgeving uit de AVG en de Wpg.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid informatiebeveiliging uiteengezet.

Hoofdstuk 3 betreft het strategisch beleid privacy. Hier wordt ingegaan op de AVG, de Wpg en andere actuele ontwikkelingen op het gebied van privacy. Hoofdstuk 4 beschrijft ten slotte hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan: het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT, maar heeft ook betrekking op de politiek, het bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Wat is privacy?

Er wordt tegenwoordig veel informatie vastgelegd, vaak zonder dat we hierbij stil staan. Bij privacy gaat het erom dat men regie houdt over de over hen vastgelegde gegevens; het gaat over zeggenschap over de eigen persoonsgegevens. Omdat wij als gemeente dagelijks te maken hebben met deze persoonsgegevens, is het noodzakelijk te voldoen aan wetgeving zoals de AVG en ook de Wet politiegegevens (Wpg).

1.4 Ambitie van de gemeente op het gebied van informatiebeveiliging en privacy

Gemeente Waalre investeert in digitale veiligheid door onze systemen up-to-date te houden. We trainen op digitale aanvallen. Cybersecurity en beveiligingschecks maken deel uit van ons dagelijks werk. We zorgen ervoor dat onze medewerkers getraind en voorbereid zijn.

"Cybersecurity, beveiligingschecks en privacy maken deel uit van ons dagelijks werk"

Gemeente Waalre ontwikkelt haar rol als (keten)partner, zowel in de regio als op landelijk vlak, waarbij samenwerken met partners (gemeenten, provincie, bedrijven en andere partijen) en het delen van informatie met die partners de uitgangspunten vormen.

Op het gebied van privacy geldt dat er continu gewerkt wordt aan het verbeteren van processen en het vergroten van het bewustzijn van alle medewerkers. De processen worden zo ingericht dat ze persoonsgegevens op een juiste manier beschermen en deze enkel worden gebruikt waar nodig. Bij nieuwe processen wordt de bescherming van persoonsgegevens standaard meegenomen. Daar waar gewenst, worden bewuste keuzes door het bestuur en management gemaakt om af te wijken van de AVG en Wpg met bijbehorende risico's en wordt dit vastgelegd in het risico register. Hierdoor is de gemeente Waalre in control op het gebied van privacy.

"De gemeente Waalre is in control op het gebied van Informatiebeveiliging en Privacy"

2 Strategisch informatiebeveiligingsbeleid

2.1 Doel

Het doel van dit beleid is richting geven en kaders stellen op het gebied van Informatiebeveiliging en Privacy. Wat zijn onze uitgangspunten, ambities en doelen en hoe willen we die bereiken tegen de achtergrond en ontwikkelingen op dit beleidsterrein. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het Jaarplan Informatiebeveiliging en Privacy.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG (Baseline Informatiebeveiliging Gemeente). Dat wil zeggen dat de organisatie nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Nieuwe versie DigiD-norm B.01

In 2022 is er een versie 3 uitgebracht van de Norm voor de ICT-beveiligingsassessments DigiD. Hierin is een extra controlepunt toegevoegd: de norm B01. Deze norm houdt in dat er in het informatiebeveiligingsbeleid specifiek aandacht wordt besteed aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.

Als bijlage is dit aanvullende webapplicatiebeleid toegevoegd aan het Strategisch Informatiebeveiligings- en Privacybeleid.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader [1] BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

[1] Deze principes worden tegelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen van de gemeente, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van gemeente Waalre. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurlijke agenda.

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is gebruikt bij het opstellen van dit beleid.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

Onze gemeente kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017 (ook wel ISO 27001 genoemd). Dit is een wereldwijd erkende norm op het gebied van informatiebeveiliging. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.

De BIO bestaat uit een baseline met verschillende niveaus van beveiligen: BBN 1 tot en met 3. Voor de lokale overheid wordt BBN2 als standaard beveiligingsniveau gehanteerd, tenzij anders aangegeven. Ook zijn/worden praktische operationele handreikingen uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.

De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het Jaarplan Informatiebeveiliging en Privacy zal deze structuur volgen.

2.4 Plaats van het strategisch beleid

Dit strategisch beleid wordt gebruikt om de basis te leggen en richting te geven voor de verdere invulling van informatiebeveiliging. Dit beleid zal worden doorvertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het Jaarplan Informatiebeveiliging en Privacy.

Daarbij wordt het beleid op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het Jaarplan Informatiebeveiliging en Privacy, vastgesteld door het Strategisch Management Team (SMT), worden deze tactische en operationele aspecten verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de Functionaris Gegevensbescherming (FG), de Chief Information Security Officer (CISO), het dreigingsbeeld van de Informatiebeveiligingsdienst (IBD) en de uitkomsten van ENSIA (= Eenduidige Normatiek Single Information Audit).

2.5 Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente Waalre en externe partijen (bijvoorbeeld politie en brandweer), het gebruik daarvan door medewerkers en

(keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch Informatiebeveiliging en privacybeleid is een algemene basis. Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten

Het bestuur en het management spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente Waalre heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele management van de gemeente Waalre geeft een duidelijke richting aan informatiebeveiliging. Ze voelen zich betrokken bij het uitdragen en handhaven van informatiebeveiliging voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het I&A-beleid van de gemeente Waalre en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging
- Adequate bescherming van bedrijfsmiddelen
- Het minimaliseren van risico's van menselijk gedrag
- Het voorkomen van ongeautoriseerde toegang
- Het garanderen van correcte en veilige informatievoorzieningen
- Het beheersen van de toegang tot informatiesystemen
- Het waarborgen van veilige informatiesystemen
- Het adequaat reageren op incidenten
- Het beschermen van kritieke bedrijfsprocessen
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers
- Het waarborgen van de naleving van dit beleid

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het bestuur en het management van de gemeente Waalre is eindverantwoordelijk voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het management. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het strategisch

informatiebeveiligingsbeleid vormt samen met het Jaarplan Informatiebeveiliging en Privacy het fundament onder een veilige informatievoorziening. In het Jaarplan Informatiebeveiliging en Privacy wordt de veiligheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. De PDCA-cyclus ('Plan, do, check en act') vormt de basis van het managementsysteem van informatiebeveiliging.
- De gemeente Waalre stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker is verplicht gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht. Bij vermeende inbreuken hiervan moet er melding van worden gemaakt. Dit geldt voor zowel vaste als tijdelijke, interne of externe medewerkers.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het College van B&W van de gemeente Waalre stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- Het SMT stelt jaarlijks het informatiebeveiligingsmeerjarenplan vast.
- Het SMT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Het SMT is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de teammanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het College van B&W en SMT.
- Tijdens de planning & control-cyclus dient er aandacht te zijn voor de informatiebeveiliging. Basis hiervoor is de rapportage van de CISO. De onderwerpen die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De teammanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging- en privacyprocessen binnen het eigen team.
- Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente Waalre en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind en voorbereid in het gebruik van beveiligingsprocedures en cybersecuritymaatregelen.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Teammanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teammanagers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met (keten)partners en leveranciers.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt er een informatiebeveiligingsplan opgesteld of herijkt onder leiding van de Chief Information Officer (CIO). Hierbij wordt verwezen naar het beleidsplan I&A van 2022. Binnen gemeente Waalre vervult de manager bedrijfsvoering deze rol.

Input voor het bovengenoemde plan zijn:

- De uitkomsten van zowel interne als externe audits;
- Het dreigingsbeeld gemeenten van de IBD;
- De door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3 Strategisch beleid Privacy

Gemeente Waalre heeft een belangrijke taak om de privacy van de burgers te waarborgen. Hiervoor is een Functionaris Gegevensbescherming (FG), een onafhankelijk toezichthouder, aangesteld bij gemeente Waalre voor zowel AVG als Wpg. De FG vormt hierbij binnen gemeente Waalre een verlengstuk van de Autoriteit Persoonsgegevens (AP), die de bescherming van persoonsgegevens bevordert en bewaakt.

3.1 Algemene Verordening Gegevensbescherming (AVG)

De Algemene Verordening Gegevensverwerking (AVG) stelt eisen aan de **verwerking en bescherming** van persoonsgegevens van natuurlijke personen en betreffende het vrije verkeer van deze gegevens binnen de Europese Unie. Dit is nodig omdat de technologie een vlucht neemt en dit knelpunten en problemen met zich meebrengt. Bijvoorbeeld met betrekking tot het omgaan met de gevolgen van nieuwe technologieën, het omgaan met de globalisering en internationale gegevensdoorgifte en de behoefte aan een samenhangend wettelijk kader voor gegevensbescherming.

De gemeente Waalre verwerkt dagelijks persoonsgegevens en doet dit doelmatig en vertrouwelijk, volgens de AVG.

3.1.1 Doel

Op grond van de Verordening moet elke verwerking van persoonsgegevens voldoen aan de volgende beginselen:

- Rechtmatig, behoorlijk en transparant: de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn;
- Doelbinding: de verwerking moet gebonden zijn aan specifieke verzameldoelen;
- Minimale gegevensverwerking: de persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is;
- Juistheid: de gegevens moeten juist zijn;
- Opslagbeperking: de gegevens mogen niet langer worden bewaard dan nodig;
- Integriteit en vertrouwelijkheid: gegevens moeten goed beveiligd zijn en vertrouwelijk blijven;

Waalre is als verwerkingsverantwoordelijke verantwoordelijk voor:

- De structurele naleving van bovenstaande AVG-beginselen door toepassen van Privacy by Design en risicoanalyses DPIA;
- Het aantonen dat een verwerking van persoonsgegevens aan deze beginselen voldoet (verantwoordingsplicht);
- Transparantie naar de betrokkenen van wie we persoonsgegevens verwerken;
- Tijdig beantwoorden van de vragen van betrokkenen ten aanzien van hun persoonsgegevens die door ons verwerkt worden (rechten van betrokkenen);
- Tijdig melden van datalekken.

Dit alles niet alleen voor onze organisatie intern, maar ook voor de externen aan wie wij taken uitbesteden of voor wie wij taken verzorgen.

Het doel van de gemeente Waalre door de AVG goed toe te passen is het risico voor de natuurlijke persoon (burger/medewerker) zoveel mogelijk te beperken.

3.1.2 Basisbeginselen AVG

De gemeente gaat op een veilige manier om met persoonsgegevens en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende beginselen:

- Rechtmatigheid, behoorlijkheid, transparantie: persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt;
- Juistheid: persoonsgegevens moeten juist en actueel zijn. Het verwerken van onjuiste persoonsgegevens kan tot grote problemen leiden en een inbreuk vormen op de persoonlijke levenssfeer. De gemeente neemt redelijke maatregelen om onjuiste persoonsgegevens te wissen en te rectificeren;
- Grondslag en doelbinding: persoonsgegevens worden alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige, in de wet geregelde, grondslag verwerkt;
- Dataminimalisatie: persoonsgegevens worden alleen verwerkt die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt;
- Bewaartermijn: persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven;
- Integriteit en vertrouwelijkheid: persoonsgegevens worden zorgvuldig en vertrouwelijk behandeld. Persoonsgegevens worden alleen verwerkt voor het doel waarvoor deze gegevens zijn verzameld. Daarbij wordt gezorgd voor passende beveiliging van persoonsgegevens;
- Delen met derden: in het geval van samenwerking met externe partijen (zoals leveranciers en ketenpartners) waarbij sprake is van gegevensverwerking van persoonsgegevens, wordt het thema Informatiebeveiliging en Privacy nadrukkelijk opgenomen in de samenwerkingsovereenkomst. In deze overeenkomst worden de doelen specifiek uitgewerkt, zijn rollen en verantwoordelijkheden duidelijk omschreven en zijn er afspraken gemaakt over de eisen waar gegevensuitwisseling aan moet voldoen. De gemeente houdt toezicht op naleving van deze afspraken;
- Subsidiariteit: voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt. Indien het doel waarvoor persoonsgegevens worden verwerkt in redelijkheid voor de bij de verwerking betrokken personen op een minder nadelige wijze kan worden verwezenlijkt, dan kiest de gemeente altijd voor die mogelijkheid;
- Proportionaliteit: de inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel;
- Rechten van betrokkenen: de gemeente respecteert alle rechten die een betrokkene toekomen vanuit de AVG, zoals het recht van: inzage, dataportabiliteit, rectificatie, beperking van de gegevensverwerking, wissen van persoonsgegevens, intrekken van de toestemming en bezwaar. De gemeenten faciliteert betrokken bij de uitoefening van hun rechten.

3.2 Wet politie Gegevens (Wpg)

Politiegegevens zijn persoonsgegevens die in het kader van de politietaak worden verwerkt. Naast de politie moeten ook andere organisaties zich aan de Wpg houden: de bijzondere opsporingsdiensten (BOD) en de buitengewoon opsporingsambtenaren (boa's). De gemeenten die boa's in dienst hebben vallen onder deze wettelijke regeling. De gemeente Waalre heeft boa's in dienst en is derhalve gehouden aan de Wpg.

3.2.1 Doel
De Wet politiegegevens (Wpg) is een wet die de rechten en de plichten van de politie zelf, maar ook die van de burger, regelt voor wat betreft het verwerken van politiegegevens.

3.2.2 Uitgangspunten Wpg
Om vast te kunnen stellen dat gemeenten bij hun verwerkingen van politiegegevens conform de wettelijke eisen hebben gehandeld, wordt een audit Wet politiegegevens uitgevoerd.

De gemeente Waalre voert als verwerkingsverantwoordelijke twee jaren na inwerkingtreding van de wet (verloopdatum op 01-01-2023), en vervolgens eenmaal in de vier jaren een externe privacy audit uit. Ter voorbereiding op de externe audit wordt jaarlijks een interne audit door de FG Wpg uitgevoerd. Die interne audit is te vergelijken met een zelfevaluatie. De interne audit (opzet, bestaan en werking) heeft betrekking op enkele onderdelen van de wet en heeft tot doel voor het onderdeel of de onderdelen van de wet waar de interne audit zich op richt, op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven.

Een buitengewoon opsporingsambtenaar (boa) heeft meerdere rollen en onder verschillende wetgevingen.
- Als toezichthouder: dan valt de verwerking van persoonsgegevens onder de AVG.
- Als opsporingsambtenaar: verwerking van persoonsgegevens valt onder de Wet politiegegevens (Wpg) en Besluit politiegegevens buitengewoon opsporingsambtenaren.

Voor Wpg gegevens (dus voor opsporing) gelden andere regels dan onder de AVG het geval zou zijn geweest. Bijvoorbeeld andere bewaartermijnen, of andere eisen die gelden bij het onderling delen van gegevens. De gegevensverwerkingen die onder de Wpg vallen krijgen andere kenmerken dan die van de AVG. Voor betrokkenen, zoals boa’s, is het duidelijk welke wetgeving gehanteerd moet worden.

3.3 Ontwikkelingen
De Functionaris Gegevensbescherming (FG) is een onafhankelijk toezichthouder en aangesteld voor zowel AVG als Wpg. De FG vormt hierbij binnen gemeente Waalre een verlengstuk van de Autoriteit Persoonsgegevens (AP) die de bescherming van persoonsgegevens bevordert en bewaakt.

Een privacyreglement en privacyverklaring zijn op de website gepubliceerd. Hierin staan de AVG-privacyrechten. Zo kunnen burgers bijvoorbeeld een verzoek indienen om vergeten te worden. Vanaf 2018 is gewerkt om te voldoen aan de eisen van de AVG en om als gemeente Waalre in control te zijn. Daarnaast gaat de Wpg in werking op 1 januari 2023. Hiervoor is er veel werk verzet en verbeterplannen gemaakt zodat we een de eerste audit aan de AP hebben kunnen overleggen. Hiermee voldoen we nog niet helemaal aan de eisen die voortvloeien uit de Wpg.

De boa’s werkzaam voor gemeente Waalre vervullen hierbij een niet eenvoudige taak, waarbij in sommige gevallen voldaan moet worden aan de AVG en in andere gevallen aan de Wpg. Dit is een complex geheel waarbij verwerking van gegevensverwerking ook nog eens kunnen verschuiven van AVG naar Wpg en terug. We voorzien dat er hier in de toekomst mogelijk veel extra hulp en ondersteuning gevraagd wordt van de FG Wpg.

Bij nieuwe technologische ontwikkelingen zoals big data en algoritmen, moet gekeken worden welke mogelijkheden er zijn en hoe deze techniek op een veilige manier kan

worden ingezet binnen de organisatie. Dit zal de komende jaren verder worden onderzocht en uitgewerkt.

Ten slotte zal Waalre in de toekomst altijd blijven acteren op nieuwe wetten en regelgeving.

3.4 Plaats van het strategisch beleid

Met dit beleid geven we richting aan acties die gericht zijn op naleving van de AVG en Wpg. Deze acties zetten wij in het Jaarplan Informatiebeveiliging en Privacy.

4 Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines (3LM). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (FG en CISO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

4.1 Aansturing: strategisch managementteam

Het strategisch MT (SMT) zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager. Het SMT zorgt dat de teammanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. Het SMT zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging en privacy een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het SMT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Zij draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen op aangeven van de CISO en FG van de gemeente. Het SMT autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacy wordt in de organisatie gezien als een integraal onderdeel van risicomanagement.

De FG en de CISO hebben een onafhankelijke positie binnen de organisatie. Voor de FG is dit zelfs bij wet geregeld. Over informatiebeveiliging en privacy wordt rechtstreeks aan de gemeentesecretaris en portefeuillehouder gerapporteerd. De burgemeester (portefeuillehouder) wordt ook betrokken bij de periodieke rapportages. In geval van crisis, ernstige gebreken of niet opvolgen van adviezen, mag de FG en/of CISO direct rapporteren/escaleren aan het college van B&W.

4.2 Uitvoering: teammanagers

Informatiebeveiliging en privacy valt ook onder de verantwoordelijkheid van de teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teammanagers rapporteren aan het SMT over de door hen tactisch en operationeel uitgevoerde informatiebeveiliging en privacy activiteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal twee keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in een teamoverleg.

Taken van de teammanagers in het kader van informatiebeveiliging en privacy zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wetgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is.
- Aansturen, begeleiden en coördinatie van de informatiebeveiligings- en privacybeheerders, die voor het eigen vakgebied verantwoordelijk zijn voor het geheel van activiteiten en taken die voortkomen uit het informatiebeveiligings- en privacybeleid

- Het binnen het eigen team uitdragen van het informatiebeveiligings- en privacybeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen. Voorbereiding en coördinatie hiervan ligt bij de CISO.

4.2.1 Informatiebeveiligings- en privacybeheerders

De informatiebeveiligings- en privacybeheerders zijn voor het eigen vakgebied verantwoordelijk voor het geheel van activiteiten en taken die voortkomen uit het informatiebeveiligings- en privacybeleid. Hieronder vallen de preventie van beveiligingsincidenten, detectie van dergelijk incidenten en het geven van adequate respons. De medewerker voert interne controles uit en let op de naleving van specifieke wet- en regelgeving.

Taken van de beveiligingsbeheerders:
- Maatregelen uit het informatiebeveiligings- en privacybeleid die voor het betreffende proces van toepassing zijn worden uitgevoerd
- Informatiebeveiligings- en privacy-incidenten registreren in het incidentenregister en deze regelmatig evalueren
- Rapporteren aan de teammanagers van incidenten, activiteiten en taken op eigen vakgebied
- Registratie van de maatregelen in het ISMS
- Rapportage binnen de planning en control cyclus op het gebied van informatiebeveiliging en privacy
- Verwerkings-en/of samenwerkingsovereenkomsten opstellen met derde partijen en deze toetsen.

4.3 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van het bestuur van de Waalre. De bestuurders en gemeentesecretaris van de gemeente Waalre zullen volgens geldende wet- en regelgeving en de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.
De CISO en de FG rapporteren gevraagd en ongevraagd over informatiebeveiliging en privacy aan de portefeuillehouder, de gemeentesecretaris en het SMT.

4.4 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging richting de gemeenteraad middels de ENSIA-systematiek. Dat betekent dat een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teammanagers. De teammanagers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Door deze verantwoording worden het bestuur van de gemeente Waalre en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Waalre informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Bijlage 1: Aanvullend webapplicatiebeleid DigiD-uitwerking norm B01

In aanvulling op dit informatiebeveiligingsbeleid (dat integraal van toepassing is op al onze DigiD-aansluitingen) zijn voor DigiD de volgende aanvullende maatregelen en verantwoordelijkheden van toepassing:

Normen:
- We conformeren ons aan de laatste door Logius gepubliceerde Norm ICT-beveiligingsassessments DigiD versie 3.0.
- Jaarlijks wordt dit normenstelsel in het kader van ENSIA door een externe auditor en CISO getoetst.
- Over deze toetsing vindt horizontaal (van college aan de raad) en verticaal (naar Logius) verantwoording plaats.

Eigenaarschap:
- Geheel in lijn met de BIO is het eigenaarschap van de DigiD-webapplicaties (de webapplicaties die de DigiD-functionaliteit als module aanroepen) belegd in de lijnorganisatie en is de betreffende strategisch manager Bedrijfsvoering eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

Functioneel beheer:
- Per DigiD-aansluiting is door de verantwoordelijk teammanager een functioneel beheerder aangewezen, die de verantwoordelijkheid heeft de door Logius opgestelde beveiligingsnormen te implementeren, controleren (middels een jaarlijkse TPM-verklaring) en bewijslast ervan op te bouwen in een auditdossier.
- Het auditdossier wordt jaarlijks aan onze externe auditor beschikbaar gesteld en bevat tenminste de contracten en servicerapportages van onze SaaS-leverancier(s) (norm B.05), de incidentprocedure en een overzicht van de incidenten (U/WA.02), de dataclassificatie (U/WA.05), bewijs dat de webapplicatie gehardend is (U/NW.06, tav DNSSEC) en de beoordeelde releases (C.08).
- Eenmaal per jaar (geagendeerd) wordt er door functioneel beheer en de CISO beoordeeld of alle autorisaties compleet en actueel zijn; hierover wordt verslag (autorisatiematrix) gedaan richting verantwoordelijk leidinggevende.

Technisch:
- Wij maken – voor wat betreft DigiD-aansluitingen - uitsluitend gebruik van cloudapplicaties die door SaaS-leveranciers worden geleverd. Derhalve wordt een groot deel van de door Logius afgekondigde normen ingevuld door de SaaS-leverancier die hiervan middels een jaarlijkse – door een onafhankelijk auditor opgestelde - TPM-verklaring verantwoording over aflegt.