Beleidskader

Informatieveiligheid en Privacy gemeente Waalre

2019-2022

GEMEENTE WAALRE

Eigenaar: CISO

Datum: 28-11-2019

Inhoud

1. Inleiding

Dit beleidskader beschrijft de informatieveiligheid en privacy voor de jaren 2019 tot 2022 en vervangt het in 2018 vastgestelde beleidskader informatieveiligheid en privacy 2018-2022.

In onze maatschappij is de digitalisering steeds meer gemeengoed. Onze gemeente gaat hierin mee, door onze inwoners en bedrijven op een hedendaagse manier onze diensten aan te bieden en onze processen steeds verder te digitaliseren.
Dit betekent dat we steeds afhankelijker worden van de beschikbaarheid en juiste kwaliteit van informatie om deze diensten goed en snel te kunnen leveren.
Want als onze informatie niet beschikbaar is of verkeerd is, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente.

Informatie moet dus adequaat beveiligd worden tegen dreigingen vanuit de maatschappij (denk aan hackers) maar ook die vanuit onze eigen organisatie en die van onze (keten)partners (denk aan ongeoorloofd toegang tot en wijzigen van gegevens). Sinds 2013 heeft Waalre ingezet op continuïteit van de beveiliging van persoonsgegevens en andere informatie door de invoering van het beleidskader informatieveiligheid en privacy, welk gebaseerd was op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

In 2020 wordt de BIG vervangen door een nieuw normenkader de landelijke Baseline Informatiebeveiliging Overheid (BIO). De BIO en de BIG verschillen in werkelijkheid niet zoveel van elkaar, beide zijn namelijk gebaseerd op de wereldwijde informatieveiligheidskaders NEN-ISO/IEC 27002:2017. De maatregelen die voor de BIG zijn getroffen zijn in het algemeen ook passend in het kader van de BIO. Een vergelijking met het verleden conform de BIG is helaas niet mogelijk, omdat de BIO een andere indeling heeft en ook een andere normering hanteert. Daarnaast maken we met de BIO de overstap naar een meer risico gestuurde aanpak, waarbij de verantwoordelijkheid van de informatieveiligheid expliciet(er) bij de lijn (afdelingsmanagers/proceseigenaren) wordt gelegd.

Dit herziene beleidskader beschrijft de strategische uitgangspunten en randvoorwaarden die door de organisatie worden gehanteerd voor de informatieveiligheid van de informatievoorziening, en is gebaseerd op de BIO. We nemen hierin mee het ‘Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten’ van de Informatie Beveiliging Dienst (IBD), dat de verwachtingen voor het heden en nabije toekomst ten aanzien van informatieveiligheid
toont.

Er was geen noodzaak om het beleidskader van Privacy aan te passen t.o.v. het kader van 2018 – 2022 omdat de AVG hierin al is opgenomen.

Het beleidskader heeft betrekking op het politieke bestuur, alle (inhuur)medewerkers, externe (keten)partners en onze burgers/bezoekers. Het beleidskader wordt één keer per 3 jaar herzien of eerder bij wijzigingen van wet- en regelgeving. De CISO zal deze herziening coördineren.

Helaas ontkomen we er niet aan in het beleidskader, om afkortingen te noemen. Deze zijn bijlage 1 overzichtelijk opgenomen.

2. Bewustwording

De wereld om ons heen staat niet stil en we zullen geconfronteerd blijven worden met nieuwe dreigingen en ontwikkelingen, zowel extern als intern. Want naast (intern) verloop van medewerkers en de komst van nieuwe technieken, blijft onze organisatie in beweging met integrale dienstverlening, nieuwe en veranderende taken, nieuwe en veranderende samenwerkingen met (keten)partners en burgers.
Om grip op bovenstaande ontwikkelingen te krijgen en houden, is en blijft bewustwording binnen de organisatie noodzakelijk. Medewerkers zijn vaak onbewust onbekwaam en zorgen zo voor dagelijkse beveiligingsrisico's en (potentiële) datalekken.

Afgelopen jaren is aan de algemene bewustwording van Waalre gewerkt, met name via berichtgeving op Intranet, het houden van een quiz en werksessies op de afdelingen, een escape room. We gaan hiermee door. Waarbij we komende periode ook expliciet(er) inzetten op de bewustwording van het Managementteam, zodat zij in staat worden gesteld hun verantwoordelijkheid ten aanzien van informatieveiligheid en privacy te nemen en deze actiever uitdragen.

Het onderwerp bewustwording zal in de uitvoeringsplannen van informatieveiligheid en privacy worden meegenomen. Hoe we bewustwording gaan meten en hierop gaan sturen zal onderdeel van de plannen zijn.

3. Beleidskader informatieveiligheid

De gemeente Waalre werkt dagelijks aan het verhogen van de betrouwbaarheid, vertrouwelijkheid en efficiency van de informatievoorziening, en werkt daarmee aan het minimaliseren van de dreigingen op het gebied van (informatie)veiligheid, onder andere door het weerbaarder maken van de digitale processen.

Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens én risicomanagement.
Risicomanagement betekent dat de lijn (afdelingsmanagers en/of proceseigenaren) meer dan vroeger op voorhand keuzes en afwegingen maken, om de informatie in bestaande en nieuwe processen ook adequaat te beveiligen.
De lijnmanager bepaalt welke kwetsbaarheden zich voor kunnen doen binnen het proces dat onder zijn/haar verantwoordelijkheid wordt uitgevoerd, bepaalt hoe groot het risico is als deze kwetsbaarheid zich manifesteert en bekijkt welke beveiligingsmaatregelen getroffen moeten worden om op een geaccepteerd risico uit te komen. Deze verantwoordelijkheid stopt niet bij de taken die intern door gemeente Waalre worden uitgevoerd, maar geldt ook voor taken die door (keten)partners worden uitgevoerd.
Als eindverantwoordelijke zal het bestuur over de risico's geïnformeerd worden. De acceptatie van risico's bij kritische en afdelingsoverstijgende processen zal aan het bestuur worden voorgelegd.
Om risicomanagement hanteerbaar en efficiënt te houden hanteert de BIO drie Basis Beveiliging Niveaus (BBN), deze worden verder uitgewerkt in 3.3.1.

De scope van dit beleidskader informatieveiligheid zijn alle processen van de gemeente en onderliggende systemen, informatie en gegevens van de gemeente en externe (keten)partners, en het gebruik daarvan door (inhuur)medewerkers en (keten)partners. Ongeacht locatie, tijdstip en gebruikte apparatuur.
Het beleidskader is de algemene basis voor de aanvullende beveiligingseisen uit specifieke wetgeving zoals Basisregistratie Personen (BRP), Paspoort Uitvoeringsregeling Nederland (PUN), Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), Basisregistratie Adressen en Gebouwen (BAG) en Digitale Identiteit (DIGID).

We onderkennen raakvlakken en dit beleidskader stemmen we af met het privacy beleid, het informatievoorzieningsbeleid, het algemene beveiligingsbeleid Huis van Waalre en het Zaakgericht Werken.

Dit beleidskader wordt aangevuld met 'onderwerp specifieke' beleidsdocumenten (op tactisch niveau) en werkinstructies (op operationeel niveau). De daaruit voortkomende maatregelen en werkzaamheden worden uitgewerkt in het jaarlijks te actualiseren informatieveiligheidsplan.

3.1. De 10 informatieveiligheid principes

Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente.
Vandaar dat de gemeente Waalre de volgende 10 informatieveiligheid principes van de IBD hanteert:

1. Bestuurders en managers bevorderen een veilige cultuur.
2. Informatieveiligheid is van iedereen.

3. Informatieveiligheid is risicomanagement (oftewel identificeer, monitor en beheers risico's).
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatieveiligheid behoeft ook aandacht in (keten)samenwerking.
6. Informatieveiligheid is een proces.
7. Informatieveiligheid kost geld (maar bespaard ons ook geld).
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur heeft de eindverantwoordelijkheid.

Deze principes beschrijven de waarden die het bestuur en management van de gemeente Waalre hanteert, en ondersteunen bij de borging van informatieveiligheid in de organisatie en met name met betrekking tot risicomanagement.

3.2. Stand van zaken

De BIO heeft 4 algemene hoofdstukken en 14 inhoudelijke hoofdstukken met in totaal 112 normen.
Voor de algemene 4 hoofdstukken zijn geen normen gesteld en worden dus geen metingen verricht.
Voor hoofdstuk 5 t/m hoofdstuk 18 staat in volgend schema ons vertrekpunt conform de BIO (op basis van de GAP-analyse die in juni – augustus 2019 is uitgevoerd).

Hoofdstukken	Aantal normen	Van deze norm behaald (BIO Score)
5 Beveiligingsbeleid	2	2
6 Organisatie	6	1 en 4 deels
7 Veilig Personeel	6	4 en 2 deels
8 Beheer bedrijfsmiddelen	10	1 en 4 deels
9 Toegangsbeveiliging	14	2 en 8 deels
10 Cryptografie	2	1
11 Fysieke beveiliging (en omgeving)	15	11 en 3 deels
12 Beveiliging bedrijfsvoering	14	4 en 5 deels
13 Communicatiebeveiliging	7	2 en 1 deels
14 Systeem aanschaf/onderhoud	12	2 en 2 deels
15 Leveranciersrelaties	5	4 deels
16 Beheer van incidenten	7	3 en 3 deels
17 Bedrijfscontinuïteit	4	2 en 1 deels
18 Naleving	8	4 deels
Totaal	**112**	**33 en 41 deels**

Tabel 1: Vertrekpunt van Waalre conform de BIO

3.3. Ambitie

Om 100% veilig te zijn en overal te voldoen aan de BIO is onmogelijk: zoals eerder geschetst verandert de wereld om ons heen (snel!) en ook onze organisatie is en blijft in beweging en daarnaast zijn we allemaal mensen die fouten kunnen en mogen maken. We streven naar een stabiele basis, zodat we kunnen werken volgens de normen en waarden van de gemeente Waalre (termen: rechtsbescherming, rechtsgelijkheid en een betrouwbare partner).

We focussen ons de komende periode op de processen of systemen waarin vertrouwelijke informatie wordt verwerkt: vanaf nu de kritische processen genoemd. Omdat deze de meeste risico's met zich meebrengen en we niet de middelen hebben om alle processen onder de loep te nemen.

We accepteren vooralsnog het risico dat minder kritische processen mogelijk minder adequaat beveiligd zijn. Maar daar waar de minder kritische processen gebruik maken van dezelfde (basis)infrastructuur, systemen, enzovoorts, liften ze mee in de genomen maatregelen voor de kritische systemen.

Ambitie voor 2022: de gemeente Waalre is in control op het gebied van informatieveiligheid

Met als eerste stap eind 2021 voor de kritische processen te voldoen aan het BIO BBN2 niveau

3.4. Uitgangspunten informatieveiligheid

Om aan deze ambitie te kunnen voldoen stellen wij voor de volgende uitgangspunten van de BIO-domeinen te hanteren:

3.4.1. Informatieveiligheidsbeleid (BIO hoofdstuk 5)

We hebben een informatieveiligheidsbeleid (dit document). Daarnaast hebben we een informatieveiligheidsplan waarin alle te ondernemen acties en bijbehorende tijdsfasering staan. Bovendien gebruiken we een Informatie Security Management Systeem (ISMS) om in control te zijn van de te nemen BIO maatregelen. Daaruit is ook tabel 1 hierboven afkomstig.

De BIO vereist dat per proces of systeem een eigenaar wordt aangewezen, die hiervoor het BBN niveau bepaalt, eventuele risico's duidt, en adequate maatregelen treft. Door inbedding van informatieveiligheid in projecten, ongeacht het project, zorgen we dat dit aan de voorkant meegenomen wordt.

De in de BIO hanteert 3 basisbeveiligingsniveaus (BBN):

- BBN2: beveiliging conform goed huisvaderschap; toont deze beveiliging een betrouwbare overheid?' Deze is voor gemeentes het belangrijkste niveau en deze wordt hieronder verder uitgelegd.
- BBN1: 'welke beveiliging mag minimaal verwacht worden conform de wet en regelgeving'? Deze norm geldt als BBN2 te zwaar wordt bevonden.
- BBN3: geldt als er departementale vertrouwelijke of vergelijkbaar vertrouwelijke informatie wordt verwerkt waarbij weerstand moet worden geboden tegen dreigingen van statelijke actoren of beroepscriminelen en waarvoor van toepassing is:

1) verlies van informatie een grote impact heeft, waarvan niet is uit te leggen als deze niet gerubriceerd en beschermd wordt op BBN3 niveau.
2) informatie met BBN3 rubricering door derden aan ons wordt geleverd.
3) aansluiting op een BBN3 infrastructuur is vereist om de informatie te kunnen verwerken.

Basisbeveiligingsniveau 2 (BBN2)
Voor processen en systemen binnen de overheid en dus ook voor de gemeente Waalre, vormt het basisbeveiligingsniveau 2 (BBN2) het uitgangspunt als het volgende van toepassing is:
1) Er vertrouwelijke informatie wordt verwerkt.
2) Mogelijke incidenten leiden tot bestuurlijke commotie.
3) Er onzekerheid bestaat of ook alle informatie van derden open(baar) is.
4) De veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

Het te beschermen belang is:
a) Vertrouwelijke informatie.
b) Privacygevoelige informatie met verhoogd vertrouwelijkheidsniveau.
c) Informatie in het kader van beleidsvorming.
d) (indien van toepassing voor de gemeente Waalre commercieel vertrouwelijke informatie).

Passende maatregelen worden genomen om te voldoen aan:
I) de wet- en regelgeving en in het bijzonder aan beveiligingseisen als gevolg van de Algemene Verordening Gegevensbescherming (AVG),
II) aansluitvoorwaarden van generieke / gemeenschappelijke diensten,
III) afhankelijkheden in ketens en netwerken,
IV) minimale eisen ten behoeve van een efficiënte beveiliging,
V) preventieve bescherming tegen dreigingen, met uitzondering van geavanceerde dreigingen afkomstig van statelijke actoren of beroepscriminelen. Hiervoor geldt dat ze worden gedetecteerd en vervolgens wordt hierop passend gereageerd.

Daar waar nodig wijkt gemeente Waalre af van het BBN2 niveau. Dit wordt bepaald door het afdelingshoofd/proceseigenaar door uitvoering van een BBN-toets per informatiesysteem, een gedeelte van het proces of het totale proces.

3.4.2. Organisatie (BIO hoofdstuk 6)
Gemeente Waalre belegt de rollen voor informatieveiligheid en privacy in de organisatie . In het kort is het als volgt vastgesteld:
De aansturing gebeurt door de gemeentesecretaris en de uitvoering is belegd bij de afdelingshoofden en eventueel verder in de lijn bij de proces- of systeembeheerders. De informatieveiligheidsorganisatie (CISO en ISO) is de tweede lijn en ondersteunt, adviseert, coördineert en bewaakt of de lijn zijn verantwoordelijkheden neemt. De (externe of interne) auditor zal de huidige situatie objectief beoordelen en eventuele verbetermogelijkheden adviseren.

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

De lijn is verantwoordelijk voor de ketens van informatiesystemen, niet alleen voor de interne processen, maar ook hetgeen we bij dienstenleveranciers en ketenpartners hebben belegd. Daar hoort ook bij het toegangsbeheer regelen en het (melden en)

oplossen van beveiligingsincidenten.
Voor interne en externe processen worden de risico's op schade (Beschikbaarheid, Integriteit, Vertrouwelijkheid) en dreigingen in beeld gebracht en leggen we beveiligingsafspraken in overeenkomsten vast. Overeenkomsten met externe partijen zijn Gemeentelijke inkoopvoorwaarden bij IT, Service Level Agreements, verwerkersovereenkomsten, etc.. Overeenkomsten met personeel zijn integriteitsverklaringen, verklaring geheimhouding, afspraken ambtseed en/of belofte, etc..

Deze risico-inschatting en het BBN niveau geven de risico's aan die we lopen, of en welke controls en (verplichte) maatregelen we moeten treffen om de risico's te beperken, en/of de afweging om eventuele (rest)risico's te accepteren.

Nieuwe processen worden ingericht conform de BIO. Voor bestaande processen bekijken we bij wijziging welke BIO controls en maatregelen getroffen moeten worden. De risicovolle zaken krijgen voorrang bij de aanpassingen.

3.4.3. Veilig personeel (BIO hoofdstuk 7)
De zorg voor informatieveiligheid en privacy ligt bij alle medewerkers, dus ook bij collegeleden en inhuur derden. Dit vraagt om duidelijke afspraken en regels bij zowel indiensttreding, tijdens dienstverband en ook bij beëindiging van het dienstverband, respectievelijk contract.

3.4.4. Beheer (bedrijfs-) middelen (BIO hoofdstuk 8)
Bij de gemeente Waalre voeren we een registratie van bedrijfsmiddelen van de hardware, telefoons en applicaties. Zo weten we wanneer er andere apparaten zich op ons netwerk/infrastructuur bevinden. Daarnaast worden de gegevens en werkprocessen geclassificeerd door de eigenaar en zo nodig qua classificatie bijgesteld (conform de VNG Realisatie dataclassificatie methodiek).

3.4.5. Toegangsbeveiliging (BIO hoofdstuk 9)
Bij de bouw van het nieuwe kantoor en de verandering van ICT-leverancier is rekening gehouden met hogere eisen aan de toegang.
De toegang tot ruimtes, applicaties, werkomgevingen, infrastructuur en mappenstructuur hebben continue monitoring nodig. Zij zijn ingericht met o.a. sterke wachtwoorden en controle op autorisaties.

3.4.6. Cryptografie (BIO hoofdstuk 10)
Cryptografie is het verbergen c.q. versleutelen van informatie.
De gemeente Waalre zorgt voor het versturen van betrouwbare digitale berichten aan personen, bedrijven, tussen systemen en voor opslag van berichten/bestanden. Door inzet van technieken zoals toegangscodes op apparatuur, versleuteling (encryptie) van mails, beveiligingscertificaten op websites.
Tevens zorgt de gemeente Waalre ervoor dat kwetsbaarheden in systemen minder snel voorkomen en misbruikt kunnen worden, door het actueel en veilig houden van systemen via een adequaat beheer van beveiligingsupdates en het uitzetten van overbodige functies (ook wel hardening genoemd).

3.4.7. Fysieke beveiliging (BIO hoofdstuk 11)
Voor de ruimtes waar informatiedragers en ICT worden gebruikt zijn voldoende maatregelen getroffen (tegen zowel natuur als menselijk handelen). Door aanbrenging van zonering en afspraken. Daarnaast zijn er afspraken ten aanzien van beveiliging en verwijdering van apparatuur gemaakt.

3.4.8. Beveiliging bedrijfsvoering (BIO hoofdstuk 12)
Om de bedrijfsvoering adequaat te laten plaatsvinden, treft de gemeente Waalre beheersmaatregelen. Ten aanzien van correcte en veilige bediening van ICT apparatuur, wijzigingen in informatiesystemen, verlies van gegevens, monitoring van gebeurtenissen (logging genoemd) en adequaat reageren op technische kwetsbaarheden (beveiligings-updates).

3.4.9. Communicatiebeveiliging (BIO hoofdstuk 13)
Afspraken worden gemaakt ten aanzien van bescherming van informatie die het netwerk van de gemeente Waalre binnenkomt of uitgaat, en over informatie die in de (Cloud)systemen zit. Dit gebeurt voor zowel intern als extern belegde diensten en wordt vastgelegd in overeenkomsten. Bijvoorbeeld in een Service Level Agreement (SLA).

3.4.10. Aanschaf/ontwikkeling/onderhoud van informatiesystemen (BIO hoofdstuk 14)
Aanschaf van (Cloud) applicaties gebeurt conform de eisen voor dataclassificatie, en deze voldoen aan de inkoopvoorwaarden (GIBIT) en de BIO. (Test) gegevens in ontwikkeling en ondersteunende processen worden ook conform de BIO beveiligd.

3.4.11. Leveranciersrelaties (BIO hoofdstuk 15)
De gemeente Waalre maakt afspraken met leveranciers die toegang hebben tot de bedrijfsmiddelen, systemen en/of informatie, legt deze vast, en zorgt voor de verantwoording hierover. Bijvoorbeeld via geheimhouding, beveiligingsafspraken/SLA of een verwerkersovereenkomst.

3.4.12. Beheer incidenten (BIO hoofdstuk 16)
Incidenten op het gebied van informatievoorziening moeten zo snel mogelijk via de juiste kanalen worden gemeld en opgelost. Het betreft zowel incidenten met betrekking tot ICT-toepassingen als analoge informatiedragers en data. De incidenten worden geregistreerd en periodiek aan de verantwoordelijke gerapporteerd.

3.4.13. Bedrijfscontinuïteit (BIO hoofdstuk 17)
Applicaties en infrastructuur worden periodiek op werking getest. Dit om de continuïteit van de bedrijfsvoering te waarborgen. Afhankelijkheden en risico's worden geïdentificeerd en de gevolgen worden in kaart gebracht.

3.4.14. Naleving (BIO hoofdstuk 18)
Kritieke applicaties en processen worden ingericht conform wet- en regelgeving, bijv. de BRP, BAG, DIGID en SUWINET. Er wordt alleen legale software gebruikt. Data en documenten worden opgeslagen conform de archiefwetgeving en gebruikt conform de privacywetgeving. De ENSIA audit en interne controles worden uitgevoerd om de naleving van de BIO te verantwoorden, op basis van opzet en bestaan. In de toekomst zal ook de werking getoetst gaan worden. Dit vereist van de gemeente dat de processen geborgd zijn. Jaarlijks zal over de audit en controles naar de lijn en het bestuur gerapporteerd worden.

3.5. Informatieveiligheidsplan

Met dit beleidskader geven we richting aan de acties t.a.v. informatieveiligheid. Deze acties zetten wij in een informatieveiligheidsplan wat jaarlijks zal worden geactualiseerd. De verbeterpunten voor 2020 treft u aan in de bijlage. Als deze verbeterpunten in 2020 worden uitgevoerd verwachten we als resultaat dat van de 112 normen er 62 zijn behaald en 24 normen deels. Dit was in 2019, 33 behaald en 41 normen deels.

4. Beleidskader Privacy

De gemeente Waalre werkt dagelijks met persoonsgegevens, deze gegevens worden doelmatig en vertrouwelijk, volgens de AVG verwerkt.

4.1. Stand van zaken

Op het gebied van privacy is in de periode van 1 mei tot en met 25 mei 2018 een stap gezet om de basis op orde te krijgen. De Functionaris Gegevensbescherming (FG) is aangesteld, een privacyreglement en privacyverklaring zijn op de website gepubliceerd en burgers kunnen een verzoek indienen om bijvoorbeeld vergeten te worden. Dit is nog niet voldoende om te voldoen aan de eisen die voortvloeien uit de AVG. De basis staat, maar de organisatie voldoet niet aan de wettelijke eisen van de AVG en dit vormt een risico bij controle door de Autoriteit Persoonsgegevens (AP).

4.1.1. Basisbeginselen AVG

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;

4.1.2. Uitvoeringstaken die voortvloeien uit de AVG

De gemeente is als verwerkingsverantwoordelijke verantwoordelijk voor de naleving van deze beginselen en moet ook kunnen aantonen dat een verwerking van persoonsgegevens aan deze beginselen voldoet (de verantwoordingsplicht). Dit betekent concreet:

#	Omschrijving	Status
1.	Er is een Functionaris gegevensbescherming aangesteld.	Gedaan
2.1	Betrokkenen worden geïnformeerd over het verwerken van de persoonsgegevens. Hiervoor wordt een privacyverklaring en -regelement op de gemeentelijke website geplaatst.	Gedaan
2.2	De privacyverklaring en het -regelement worden jaarlijks bijgehouden.	Gedaan
2.3	Betrokkenen worden geïnformeerd over de verwerking van de persoonsgegevens bij het contact met de organisatie.	Gedeeltelijk
3.1	Er zijn procedures vastgesteld voor (vermoedelijke) datalekken.	Gedaan
3.2	De procedures datalekken zijn bekend in de organisatie.	Gedeeltelijk
3.3	De procedures datalekken worden bijgehouden op basis van regelgeving.	Gedaan
3.4	In het geval van een datalek wordt er melding gemaakt bij de Autoriteit Persoonsgegevens en onder bepaalde omstandigheden ook bij de betrokkenen.	Gedaan

3.5	Er is een incidentenregister datalekken.	Gedaan
3.6	Het incidentenregister datalekken wordt actief bijgehouden.	Gedaan
4.1	Er is een procedure vastgesteld voor de uitoefening van de rechten door betrokkenen.	Gedaan
4.2	De procedure en rechten van betrokkenen zijn bekend in de organisatie.	Gedeeltelijk
4.3	De procedure wordt bijgehouden op basis van relevante regelgeving.	Gedaan
4.4	Er wordt bijgehouden hoeveel verzoeken van betrokkenen er worden ontvangen.	Gedaan
5.1	De organisatie heeft een register van alle verwerkingsactiviteiten binnen de organisatie	Gedeeltelijk
5.2	Het verwerkingsregister wordt structureel bijgehouden.	Gedeeltelijk
6.1	Er is een procedure vastgesteld voor het sluiten van de verwerkersovereenkomsten en een model verwerkersovereenkomst.	Gedaan
6.2	De procedure en het model verwerkersovereenkomst zijn bekend in de organisatie.	Gedeeltelijk
6.3	De procedure en het model verwerkersovereenkomst wordt bijgehouden op basis van relevante regelgeving.	Gedaan
6.4	Met alle verwerkers van de gemeente zijn verwerkersovereenkomsten gesloten.	Gedeeltelijk
7.1	Voorafgaand aan risicovolle verwerkingsactiviteiten wordt een DPIA (Data Protection Impact Assessment) uitgevoerd.	Gedeeltelijk
7.2	Met terugwerkende kracht worden op risicovolle verwerkingsactiviteiten DPIA's uitgevoerd.	Gedeeltelijk
7.3	De Autoriteit Persoonsgegevens wordt bij bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit geraadpleegd.	Nog niet voorgekomen
8.1	Bij de inrichting van processen wordt er rekening gehouden met de principes van privacy door ontwerp (privacy by design) en standaardinstellingen (privacy by default).	Gedeeltelijk
8.2	Met terugwerkende kracht worden processen en systemen aangepast aan de hand van de principes privacy door ontwerp en standaardinstellingen.	Gedeeltelijk
8.3	Er zijn passende beveiligingsmaatregelen aanwezig met het oog op de bescherming van persoonsgegevens.	Gedeeltelijk
9.	De organisatie verleent medewerking aan de Autoriteit Persoonsgegevens.	Nog niet voorgekomen

4.2. Ambitie

Er wordt continu gewerkt 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 directie gemaakt om af te wijken van de AVG met bijbehorende risico's. Hierdoor is de gemeente Waalre vanaf 2021 in control op het gebied van privacy.

De kanttekening: binnen de AVG is er nog veel grijs gebied met betrekking tot de interpretatie van de Verordening en het is onduidelijk waar de AP de meeste aandacht op zal vestigen. De komende jaren zal aan de hand van uitspraken van de AP er steeds meer richting gegeven worden en zullen normen verschuiven. 100% voldoen aan de AVG is dan ook een utopie.

Ambitie voor 2021: de gemeente Waalre is in control op het gebied van Privacy

4.3. Uitgangspunten voor Privacy

Om aan deze ambitie te voldoen hanteren we de AVG, de Uitvoeringswet AVG en uitspraken van de AP als uitgangspunten voor het beleidskader privacy van de gemeente Waalre. De belangrijkste concepten hieruit zijn in paragraaf 4.1 beschreven.

4.3.1. Start AVG

In 2018 en in de eerste 2 kwartalen van 2019 wordt inzichtelijk gemaakt welke persoonsgegevens, waar en door wie worden verwerkt. Dit wordt geregistreerd in een verwerkingsregister (*uitvoeringstaak 5.1*).
Met partijen die namens de gemeente Waalre persoonsgegevens verwerken wordt een verwerkersovereenkomst opgesteld (*uitvoeringstaak 6.4*).
Betrokkenen kunnen hun rechten op basis van de AVG uitoefenen. Deze processen zijn ingericht en bekend binnen de organisatie (*uitvoeringstaak 4.1 + 4.2*).
De procedure datalekken is ingericht en bekend binnen de organisatie.
De uitgangspunten uit dit stuk vormen het privacybeleidskader van de gemeente Waalre en deze uitgangspunten zijn bekend binnen de organisatie (*uitvoeringstaak 3.1 t/m 3.6*).
Ook bewustwording voor privacy en bijkomende procedures is onderdeel van de uitvoering. Dit wordt zoals in hoofdstuk 2 beschreven integraal met informatieveiligheid opgepakt (*uitvoeringstaak 2.3; 3.2; 4.2; 6.2; 8.1*).

4.3.2. Ontwikkeling

In 2019 wordt er gestart met het uitvoeren van Data Protection Impact Assessments (DPIA) bij processen met een hoog risico (denk aan het CMD en het zaaksysteem) (*uitvoeringstaak 7.2*).
Bij nieuwe applicaties, processen, projecten of aanbestedingen wordt privacy als integraal onderwerp bij de ontwikkeling meegenomen (*uitvoeringstaak 7.1*). Hierbij hanteren we de principes privacy by design en privacy by default (*uitvoeringstaak 8.1*). Dit betekent dat data uitwisseling geminimaliseerd wordt tot hetgeen wat nodig is voor het uitvoeren van de taak en de standaard instellingen zo privacyvriendelijk mogelijk worden ingesteld. Ook bestaande processen en applicaties worden zo veel mogelijk geoptimaliseerd door gebruik te maken van deze twee principes (*uitvoeringstaak 8.2*).

4.3.3. Doorontwikkeling

2020 en 2021 staan in het teken van het afronden van de acties uit 2019 en het evalueren en doorontwikkelen van processen, richtlijnen en afspraken. Er worden DPIA's uitgevoerd. Er worden nieuwe prioriteiten gesteld op basis van opgedane ervaringen in 2018 en 2019 en ontwikkelingen binnen de AVG.

4.3.4. Privacy planning

Met dit beleidskader geven we richting aan de acties t.a.v. privacy. Deze acties zetten wij in een Privacy planning die jaarlijks zal worden geactualiseerd.

Bijlage 1: afkortingen lijst

Afkorting	Uitleg
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BAG	Basisadministratie Adressen en Gebouwen
BBN	Basis Beveiliging Niveaus
BGT	Basisregistratie Grootschalige Topografie
BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
BRP	Basisregistratie Personen
CISO	Chief Information Security Officer
CMD	Centrum voor Maatschappelijke Deelname
DIGID	Digitale identiteit
DPIA	Data Protection Impact Assesment
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
GIBIT	Gemeentelijke Inkoopvoorwaarden Bij IT (Informatie Technologie)
IBD	Informatie Beveiliging Dienst
ICT	Informatie en Communicatie Technologie
ISMS	Informatie Security Management Systeem
IT	Informatie Technologie
NEN-ISO/IEC 27002:2017	Wereldwijde normering mbt informatiebeveiliging NEN : Nederlandse Norm ISO: Internationale Organisatie voor Standaardisatie IEC: International Electrotechnical Commission
PSO	Privacy en Security Officer
PUN	Paspoort Uitvoeringsregeling Nederland
SLA	Service Level Agreement
SUWI	Structuur Uitvoeringsorganisatie Werk en Inkomen
VNG	Vereniging van Nederlandse Gemeenten

Bijlage 2: verbeterpunten Informatieveiligheid 2020

Hoofdstukken	Aantal normen	% BIO Score Augustus 2019	Verbeterpunten naar aanleiding van de BIO 0-meting/gap analyse jan-aug 2019
5 Beveiligingsbeleid	2	2	Uitbreiding BIO: risicomanagement opzetten en borgen.
6 Organisatie	6	1 en 4 deels	Explicieter in BIO: explicietere lijn(proces) verantwoordelijkheid. Risicoanalyses worden uitgevoerd voor kritische processen en systemen. Openstaande actie: telewerkbeleid en beleid mobile apparatuur. ENSIA2018: mobiele RAAS systeem, en werkinstructies/procedures als buiten vertrouwde omgeving wordt gewerkt (hfst 12) Voortzetten van de bewustwordingscampagne.
7 Veilig Personeel	6	4 en 2 deels	Continue actie: bewustwording. Openstaande actie: verbeteren proces in- en uitdiensttreding of personele wijzigingen. ENSIA2018 verbeterpunt bij BRP/PUN
8 Beheer bedrijfsmiddelen	10	1 en 4 deels	Openstaande acties: informatieclassificatie, actuele inventarisatielijst van bedrijfsmiddelen, passende beveiligingsmaatregelen bij uit dienst en verwijdering van bedrijfsmiddelen
9 Toegangsbeveiliging	14	2 en 8 deels	Verder verbeteren van toegangsbeveiliging, herzien van het wachtwoordbeleid
10 Cryptografie	2	1	NIEUW: Cryptografiebeleid opstellen, vaststellen en implementeren
11 Fysieke beveiliging (en omgeving)	15	11 en 3 deels	Beleid clear desk/screen opstellen, vaststellen en implementeren
12 Beveiliging bedrijfsvoering	14	4 en 5 deels	Openstaande acties: verbeteren diverse ICT-processen (wijzigingsbeheer, back-ups, logging, capaciteitsbeheer, bedieningsinstructies, audittests, verantwoording).
13 Communicatiebeveiliging	7	2 en 1 deels	UITGEBREID: verbeteren van beveiliging van netwerk(diensten) en informatietransport
14 Systeem aanschaf/onderhoud	12	2 en 2 deels	Als er een testomgeving is, dan plannen opstellen en daarin beveiliging van gegevens meenemen. ENSIA2018: gegevensclassificatie/DPIA uitvoeren
15 Leveranciersrelaties	5	4 deels	Risicoanalyse uitvoeren voor inkoop/uitbesteding. Borgen van beveiligingsafspraken en privacy by design/default in het inkooptraject en rapportering gedurende de looptijd van het contract
16 Beheer van incidenten	7	3 en 3 deels	Het informatiebeviligingsincidenten proces uitbreiden met Responsible disclosure. Het opstellen van een incidentrapportage
17 Bedrijfscontinuïteit	4	2 en 1 deels	Uitwijktest en Calamiteitenplan onderhouden en testen. BAG/BGT toevoegen. GEO omgeving stabiliseren
18 Naleving	8	4 deels	NIEUW: Verplichting een ISMS geïmplementeerd te hebben, waar de beheerders mee werken. Verantwoording via ENSIA, en voldoen aan de ENSIA 2019. Kwetsbaarheidsanalyse/pentest.