FG jaarverslag 2023

Gemeente Deurne

Inleiding

- De gemeente Deurne beschikt over veel (vaak gevoelige) persoonsgegevens van haar inwoners, medewerkers en andere relaties (betrokkenen). Zij moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig omgaat met deze persoonsgegevens.

- De interne toezichthouder, de Functionaris Gegevensbescherming (FG), houdt binnen de gemeente onafhankelijk toezicht op de naleving van wet- en regelgeving voor persoonsgegevensbescherming zoals de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

- Via dit jaarverslag brengt de FG verslag uit aan het hoogste leidinggevende niveau van de gemeente, zijnde de gemeentesecretaris, het college van Burgemeester en Wethouders en de gemeenteraad.

- Dit jaarverslag geeft inzicht in zijn bevindingen en is opgesteld in januari 2024.

Bijlagen

1. Overzicht datalekken 2023
2. Overzicht DPIA's*
3. Opvallende nieuwsfeiten 2023
4. Overzicht AVG borgingsproduct 3.0

* *Een DPIA (Data Protection Impact Assessment) geeft inzicht in privacyrisico's voor betrokkenen en welke maatregelen de gemeente kan nemen om die risico's te verkleinen of zelfs weg te nemen.*

Deel 1

Terugblik op 2023

- In 2023 zijn er stappen ondernomen om door te groeien in volwassenheid op het gebied van persoonsgegevensbescherming. Diverse aanbevelingen uit het FG jaarrapport 2022 zijn opgepakt. Bijvoorbeeld:
  - het privacybeleid is geactualiseerd;
  - een nieuwe werkwijze voor het systematisch toetsen en vastleggen van processen met persoonsgegevens is opgezet;
  - een overzicht van verwerkersovereenkomsten is gemaakt en er is een start gemaakt met het herstel van deze overeenkomsten waarin tekortkomingen zijn geconstateerd.

- In 2023 werd intern gebruik gemaakt van het AVG Borgingsproduct 3.0 van de Vereniging Nederlandse Gemeenten (VNG) als hulpmiddel om meer inzicht te krijgen in hoeverre de gemeente in staat is om de naleving van de AVG te waarborgen. Er zijn diverse verbeterslagen gemaakt in 2023. Begin januari 2024 was de uitkomst 78%. Zie bijlage 4.

- Diverse bewustwordingsactiviteiten voor medewerkers zijn georganiseerd.

- Eind 2023 werd met o.a. de burgemeester, gemeentesecretaris en managers nagedacht over (bestuurlijke) dilemma's rondom cybercriminaliteit.

- De gemeente Deurne had in 2023 als een van de weinige Nederlandse gemeenten de beveiliging van haar webdiensten helemaal op orde volgens de website basisbeveiliging.nl.

Bevindingen van de FG over 2023

Beleid

- Het oude privacybeleid stamt uit mei 2018. Deze is in 2023 geactualiseerd. Het nieuwe privacybeleid bevat een governancemodel op basis van het "Three Lines Model" waarin de taken en verantwoordelijkheden voor bescherming van persoonsgegevens per functie beschreven staan. Tevens is in het beleid toegevoegd de gemeentelijke verwerking van politiegegevens (Wpg). Het nieuwe privacybeleid dient begin 2024 nog vastgesteld en intern gecommuniceerd te worden.

Processen

Nieuwe en gewijzigde processen met persoonsgegevens

- Voordat de gemeente begint met een nieuw of gewijzigd proces waarin persoonsgegevens verwerkt worden (verwerkingen), moet ze aantoonbaar toetsen of de verwerking aan de AVG-beginselen voldoet; Mag dit? Is het doel duidelijk en gerechtvaardigd? Is het noodzakelijk? Kan het met minder? Zijn de gegevens juist? Hoe blijven ze actueel? Hoe lang moeten de gegevens bewaard worden? Is de beveiliging goed geregeld? En is de verwerking voor de burger of medewerker transparant en voorzienbaar?
- In 2023 is de gemeente gestart met het opzetten van een nieuwe werkwijze voor het toetsen en vastleggen van (nieuwe en gewijzigde) processen met persoonsgegevens en risicobeheersing. Zo zijn er procedures (deelprocessen) opgesteld voor het toepassen van privacy by design, het beheren van het verwerkingsregister en het uitvoeren van (pre-)DPIA's. Centrale registratie en toewijzing van risicobeperkende maatregelen moet de monitoring en opvolging van deze maatregelen gaan ondersteunen. Hiervoor wordt het systeem Cybermanager ingezet.

Bestaande processen met persoonsgegevens

- Het is voor de gemeente onduidelijk of de AVG-beginselen aantoonbaar in alle bestaande (risicovolle) processen (waaronder gegevensverstrekkingen) voldoende zijn geborgd.
- De FG ziet het daarom als een prioriteit dat bestaande risicovolle verwerkingen snel in kaart worden gebracht en getoetst. In 2023 is gestart met een overzicht te maken van bestaande risicovolle verwerkingen. Er is nog geen plan van aanpak gemaakt voor het toetsen van deze processen via DPIA's in de komende jaren.

Uitgevoerde DPIA's in 2023

- Twee nieuwe DPIA's zijn uitgevoerd door de gemeente Deurne zelf in 2023. Drie bestaande DPIA's zijn herzien. Alle DPIA's voldoen aan de AVG-vereisten. Zie bijlage 2.

Organisatorische inbedding

Proceseigenaarschap

- In het nieuwe privacybeleid staat een governancemodel beschreven met daarin taken en verantwoordelijkheden van proceseigenaren. Bepaalde taken en verantwoordelijkheden worden toegewezen aan procesbeheerders.
- Proceseigenaren zijn eindverantwoordelijk voor de bescherming van de (persoons)gegevens in hun processen, niet de Privacy Officer (PO), CISO (Chief Information Security Officer) of FG. Procesbeheerders zijn uitvoerend verantwoordelijk.

Bewustwording voor medewerkers

- Nieuwe medewerkers kregen in 2023 binnen 2 maanden na indiensttreding een bewustwordingstraining van de CISO over gegevensbescherming.
- In 2023 werden via de gemeentelijke leeromgeving voor medewerkers (BROS-academie) diverse e-learnings aangeboden over gegevensbescherming.
- Een Mystery Guest werd ingeschakeld. Diens bevindingen waren voor de gemeente aanleiding om extra beveiligingsmaatregelen te nemen.
- Ook andere bewustwordingsactiviteiten zijn georganiseerd zoals een cyberescaperoom en phishingtests.
- Medewerkers van de gemeente Deurne krijgen voortaan een extra tekstwaarschuwing na ontvangst van een verdachte mail.

Opschonen gegevens

- Wat er niet is, kan ook niet gelekt worden. Veel (persoons)gegevens worden onnodig bewaard op het netwerk zoals in mailboxen. Dat kan leiden tot ernstige datalekken. Zo werd bijvoorbeeld in 2023 bekend dat buurgemeente Asten in 2022 was getroffen door een cyberaanval. Medewerkers hadden geklikt op een link in een mail van de aanvallers. Daardoor kregen de aanvallers toegang tot 2 mailboxen met daarin zo'n 23.000 bestanden en gegevens van 612 inwoners.
- Voor het tijdig archiveren en schoning van persoonsgegevens is het proces bewaar archivering en vernietiging van persoonsgegevens beschikbaar gesteld aan kwaliteitsmedewerkers.

Rechten van betrokkenen

Inwoners, werknemers en relaties van de gemeente (betrokkenen) hebben het recht om na te gaan wat de gemeente doet met hun persoonsgegevens. De gemeente informeert hen hierover en zorgt ervoor dat zij controle kunnen houden over deze gegevens. Bijvoorbeeld door op verzoek inzage te bieden.

- In 2023 is 1 AVG-verzoek geregistreerd in het gemeentelijk zaaksysteem.
- De FG heeft in 2023 geen privacyklachten van betrokkenen ontvangen.
- De privacyverklaring op de gemeentelijke website en de procedure rechten van betrokkenen bevat nog geen informatie over de gemeentelijke verwerking van politiegegevens.
- Een interne privacyverklaring is vastgesteld. De OR is geïnformeerd.

Samenwerking

De gemeente werkt veel samen met derde partijen. Daarbij worden persoonsgegevens gedeeld. Het buiten de eigen deur plaatsen van taken ontslaat de gemeente niet van verantwoordelijkheid voor de gegevens. Het is belangrijk dat ook derde partijen zorgvuldig omgaan met verstrekte gegevens en dat daar afspraken over worden gemaakt. Zo is een verwerkersovereenkomst verplicht bij verstrekking van persoonsgegevens aan een verwerker.

- Een overzicht van bestaande verwerkersovereenkomsten met derde partijen is in 2023 gemaakt. Door de Privacy Officer is in 2023 gecontroleerd of deze afspraken correct en actueel zijn.
- Uit deze controle bleek dat er in het merendeel van de verwerkersovereenkomsten tekortkomingen zaten. Herstel van deze afspraken is gestart. Andere afspraken met derde partijen zijn niet gecontroleerd.

Informatiebeveiliging

Passende technische en organisatorische informatiebeveiligingsmaatregelen zijn nodig om (persoons)gegevens te beveiligen. Hierdoor worden datalekken voorkomen.

- Vanaf 2020 is door de gemeente elk jaar beter voldaan aan het basisniveau voor informatiebeveiliging (BIO; Baseline Informatiebeveiliging Overheid). Dat blijkt uit de jaarlijkse zelfevaluatie (ENSIA).
- Risico-analyses bij nieuwe projecten en de aanschaf van systemen en applicaties worden standaard uitgevoerd. Hierdoor heeft de gemeente in beeld welke technische en organisatorische beveiligingsmaatregelen noodzakelijk zijn om een passend beschermingsniveau te kunnen realiseren.
- In 2024 zal een systeem voor Monitoring, Detectie & Response (MDR) geïntroduceerd worden om het opslaan en analyseren van logging mogelijk te maken. Voor deze verwerkingen is een DPIA uitgevoerd. Logging maakt o.a. onderzoek mogelijk naar signalen van kwaadwillende manipulatie (bijv. hacking en fraude) en misbruik van bevoegdheden.
- Medewerkers dienen tijdig op de hoogte te worden gebracht dat hun handelingen in systemen worden gelogd.

Verantwoording

- Op dit moment kan de gemeente onvoldoende aantoonbaar maken dat zij voldoet aan haar AVG-verplichtingen (verantwoordingsplicht). Er is geen overzicht gemaakt van alle risicovolle processen met persoonsgegevens.

- In 2023 is geïnventariseerd welke processen met persoonsgegevens (verwerkingen) er zijn. Nieuwe of gewijzigde verwerkingen zijn in 2023 toegevoegd aan het verwerkingsregister en getoetst op rechtmatigheid. Het verwerkingsregister is in het verleden onvoldoende onderhouden waardoor het register nog onbetrouwbaar is.

- De gemeente is verplicht een datalekregister op te stellen en bij te houden. Met het datalekregister kan de gemeente aan de Autoriteit Persoonsgegevens (AP) laten zien dat zij zich houdt aan de meldplicht datalekken. De gemeente mag zelf bepalen welke vorm het register heeft, zolang zij maar de wettelijke verplichte informatie erin opneemt. Denk aan de feiten over het datalek, zoals de oorzaak, wat er precies is gebeurd en om welke persoonsgegevens het gaat, de gevolgen van het datalek en de corrigerende maatregelen die zijn genomen. De gemeente heeft een datalekregistratie. De FG constateert na onderzoek dat datalekken duidelijker, volledieger en overzichtelijker geregistreerd kunnen worden. Tijdige interne melding van datalekken door medewerkers kan ook verbeterd worden.

Wet Politiegegevens (Wpg)

De gemeente is werkgever van een buitengewoon opsporingsambtenaar (BOA) in het domein Onderwijs. Deze verwerkt politiegegevens bij de uitvoering van diens opsporingstaak. De gemeente moet daarom rekening houden met de verplichtingen uit de Wet Politiegegevens (Wpg).

- Eén van de Wpg-verplichtingen is een externe audit laten uitvoeren om de 4 jaar. De gemeente heeft dat in 2022 gedaan en het Wpg-auditrapport werd op tijd ingeleverd bij de toezichthouder, de Autoriteit Persoonsgegevens.
- Uit de externe Wpg-audit kwamen diverse verbeteracties. De gemeente heeft hiervoor een verbeterplan opgesteld. Deze is in 2023 deels uitgevoerd.
- Eind 2023 heeft de interne Wpg-audit en hercontrole plaatsgevonden door de externe auditor. De planning is om het auditrapport van de hercontrole uiterlijk 1 maart 2024 in te leveren bij de Autoriteit Persoonsgegevens (AP). Dat is toegestaan omdat de AP de uiterste inleverdatum heeft verlengd naar 1 maart 2024.
- Politiegegevens leerplicht worden door de gemeente verwerkt in het leerplichtsysteem (JVS) dat beheerd wordt door de gemeente Eindhoven. Deze gemeente heeft ook procesbeschrijvingen Absoluut en Relatief verzuim opgesteld in september 2023 en gedeeld met de regiogemeenten.
- Er is door de gemeente een auditplan Wet politiegegevens 2023-2025 gemaakt en uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens.
- In 2023 zijn er door de BOA leerplicht geen politiegegevens verwerkt.

Bijlage 1 Overzicht datalekken 2023

	Datalek
1	Een uitnodiging voor een overleg is aan een verkeerde (externe) ontvanger gestuurd.
2	Een mail van een inwoner is doorgestuurd naar een externe ontvanger in plaats van naar een collega.
3	Een bestand met NAW-gegevens van inwoners stond 2 jaar lang openbaar op de gemeentelijke website.
4	Voor een sollicitant waren CV's van andere sollicitanten inzichtelijk.
5	Een mail is verzonden naar een verkeerde ontvanger.
6	Een verwerker had onbedoeld in een groepsmail de naam en het zakelijk mailadres van een medewerker van de gemeente verstuurd.
7	Er zijn vertrouwelijke documenten gevonden in open kasten in een ruimte die alleen toegankelijk is voor geautoriseerde personen.
8	Onbevoegde toegang tot een toepassing werd geconstateerd waardoor toegang was tot namen en zakelijke contactgegevens van enkele medewerkers.

FG analyse

De gemelde datalekken gingen over persoonsgegevens die onbedoeld terecht zijn gekomen bij onbevoegden. Veelal veroorzaakt door onzorgvuldigheid en in de meeste gevallen werd het risico voor betrokkenen ingeschat als beperkt of verwaarloosbaar. In 2023 is 1 datalek gemeld aan de Autoriteit Persoonsgegevens. Er zijn corrigerende en eventuele preventieve maatregelen getroffen.

In het bewustwordingsprogramma voor medewerkers is in 2023 aandacht geschonken aan het melden en voorkomen van datalekken. Zo zijn videobeelden gemaakt en intern gedeeld waarin de burgemeester, de FG en enkele medewerkers het belang van melden van datalekken benadrukten. Het aantal gemelde datalekken was beperkt. De FG raadt de gemeente daarom aan om te gaan onderzoeken of medewerkers nog belemmeringen ervaren om datalekken te melden en zo ja, aanvullende maatregelen te nemen.

Datalekken	2018	2019	2020	2021	2022	2023
Gemeld aan de gemeente	8	10	15	13	12	8
Gemeld aan de Autoriteit Persoonsgegevens	3	5	4	4	4	1

Bijlage 2 Overzicht DPIA's

Onderwerp DPIA	Status eind 2023
Wvggz (Wet verplichte geestelijke gezondheidszorg)	DPIA uit 2019. Herzien in 2023.
Zorg- en veiligheidshuis (ZVH)	DPIA uit 2019. Herzien in 2023.
Cameratoezicht Parkeergarage Wolfsberg	DPIA uit 2020. Herzien in 2023.
Cameratoezicht gemeentehuis	DPIA uit 2021.
Jongeren in kwetsbare posities (JIKP)	DPIA uit 2021.
Agressieprotocol	DPIA uit 2022.
GPS tracker op voertuigen buitendienst	DPIA uit 2022.
Nieuwe Wet inburgering	DPIA uit 2022.
Jeugdhulpverlening	DPIA uit 2022.
Financieel systeem	DPIA uit 2022. Nog in behandeling.
Beschermd Wonen / Beschermd Thuis	DPIA uit 2022. Uitgevoerd door de Gemeenschappelijke Regeling Peelgemeenten.
BRP-koppeling Onview	DPIA uit 2022. Uitgevoerd door de Gemeenschappelijke Regeling Peelgemeenten.
Logging	DPIA uit 2023.
Vroegsignalen Schuldhulpverlening	DPIA uit 2023.
Toezicht en rechtmatigheid WMO/Jeugd	DPIA uit 2023. Uitgevoerd door de Gemeenschappelijke Regeling Peelgemeenten.
Cliëntervaringsonderzoek WMO/Jeugd	DPIA uit 2023. Uitgevoerd door de Gemeenschappelijke Regeling Peelgemeenten.

Bijlage 3 Opvallende nieuwsfeiten 2023

	Nieuwsfeiten
1 jan 2023	Wet bevorderen integriteit en functioneren decentraal bestuur is in werking getreden met uitzondering van het onderdeel geheimhouding. Die treedt in werking op 1 april 2023. Met deze wet is voor onder meer aankomende wethouders een VOG (Verklaring Omtrent Gedrag) bij hun benoeming verplicht. Ook is duidelijker wanneer er sprake is van belangenverstrengeling en wat toegestaan is op het vlak van nevenfuncties.
12 jan 2023	Autoriteit Persoonsgegevens kondigt aan dat zij gaat optreden tegen boa-werkgevers (boa = buitengewoon opsporingsambtenaren) die het verplichte Wpg-auditrapport niet toestuurden voor 1 januari 2023.
16 jan 2023	Start nieuwe taak van de Autoriteit Persoonsgegevens: algoritmetoezicht
27 jan 2023	De Wet aanpak meervoudige problematiek in het sociaal domein (Wams) is bij de Tweede Kamer ingediend. Met dit wetsvoorstel kan ervoor gezorgd worden dat gemeenten en andere betrokken organisaties die deze gezinnen helpen, makkelijker gegevens kunnen uitwisselen.
1 febr 2023	Het afschermen van het bezoekadres van politieke ambtsdragers en hun partners en huisgenoten in het Handelsregister is nu mogelijk. Dit is van belang voor politieke ambtsdragers zoals burgemeesters, wethouders en raadsleden met een eigen onderneming.
10 febr 2023	Overheden hebben meer aandacht voor naleving privacynormen, maar vanzelfsprekend is het nog niet. Dat blijkt uit onderzoek van Pro Facto en Hooghiemstra & Partners, in opdracht van het WODC. Sinds de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) in 2016 hebben overheden veel gedaan om zorgvuldiger om te gaan met persoonsgegevens. Toch is verdere verbetering zeker mogelijk en nodig, met name bij gemeenten en ministeries.
1 maart 2023	Gemeente Eindhoven staat onder toezicht van de Autoriteit Persoonsgegevens vanwege ondermaatse privacybescherming.
15 maart 2023	Gemeente Krimpen aan den Ijssel werd eind 2022 slachtoffer van CEO-fraude. Er werd EUR 176.040 overgemaakt naar buitenlandse criminele bankrekeningen.
21 maart 2023	De Eerste Kamer heeft het wetsvoorstel digitale overheid aangenomen. De Wet digitale overheid (Wdo) wordt op 1 juli 2023 in fases ingevoerd. Doel is het regelen van veilige en betrouwbare inlogsystemen voor Nederlandse burgers en bedrijven bij de (semi-)overheid.
13 april 2023	Bericht Eindhovens Dagblad. De gemeente Helmond kreeg in 2022 te maken met een cyberaanval, maar daarbij werden geen persoonsgegevens gestolen.
12 mei 2023	Uitspraak rechtbank: gemeente Hof van Twente is zelf schuldig aan de hack in december 2020. De EUR 4,2 miljoen aan herstelkosten kan niet verhaald worden op de softwareleverancier. De gemeente moet daarnaast ook de proceskosten van het kort geding, ruim EUR 20.000, betalen.
22 mei 2023	De gemeente Asten maakt bekend dat zij is getroffen door een digitale inbraak. Dat gebeurde in oktober 2022, maar de gemeente maakte het 22 mei 2023 pas bekend. Dit omdat het in eerste instantie enkel leek te gaan om een digitale inbraak met als doel factuurfraude. Pas later zou zijn gebleken dat er toegang was tot 2 mailboxen met daarin zo'n 23.000 bestanden en andere gegevens, zoals NAW- en contactgegevens, bankrekeningnummers, burgerservicenummers, kopieën van rijbewijzen, identiteitskaarten en paspoorten.

Bijlage 3 Opvallende nieuwsfeiten 2023

	Nieuwsfeiten
25 mei 2023	Nederlanders vertrouwen hun overheid steeds minder met persoonsgegevens. Dat blijkt uit het Privacy Marktonderzoek 2023 van KPMG. In de afgelopen vijf jaar is het aantal burgers met vertrouwen gedaald van 32 procent naar 19 procent.
7 juni 2023	Vorig jaar kreeg de Autoriteit Persoonsgegevens (AP) ruim 21.000 meldingen over datalekken. Meer dan 1.800 lekken waren het gevolg van cyberaanvallen.
14 juni 2023	Het Europees parlement heeft ingestemd met het AI-wetsvoorstel dat de Europese Commissie in 2021 presenteerde. Deze AI-wet moet mensen beschermen tegen de gevaren van de opmars van kunstmatige intelligentie.
15 juni 2023	Autoriteit Persoonsgegevens (AP) verlengt verscherpt toezicht gemeente Eindhoven. Hoelang de gemeente Eindhoven nog onder verscherpt toezicht blijft staan, is onbekend. Als de Autoriteit Persoonsgegevens geen verbetering ziet, kan ze besluiten om een onderzoek in te stellen. Mochten er tijdens het onderzoek overtredingen worden begaan, dan kan de toezichthouder een dwangsom of boete opleggen.
11 juli 2023	De Eerste Kamer heeft de Wet bevorderen samenwerking en rechtmatige zorg (Wbsrz) aangenomen. Doel is betere samenwerking en gemakkelijker gegevens uitwisselen om fraude in de zorg te voorkomen. De Wbsrz regelt de mogelijkheid voor partijen (waaronder gemeenten) en het Informatieknooppunt Zorgfraude (IKZ) om fraudesignalen aan te leveren en te verwerken, het instellen van het Waarschuwingsregister zorgfraude en het uitwisselen van gegevens voor het verder doen van onderzoek naar fraude.
15 sept 2023	De gemeente Alkmaar is slachtoffer geworden van ceo-fraude, waarbij het EUR 236.000 aan cybercriminelen heeft overgemaakt.
25 sept. 2023	De Data Governance Act (DGA) is van toepassing. Deze verordening (directe werking) geeft een raamwerk om (overheids-)data delen eenvoudiger te maken en hergebruik te stimuleren. Verder regelt de verordening het delen van gegevens door burgers of organisaties via een databemiddelingsdienst en bevat de verordening regels om het vrijwillig delen van gegevens te stimuleren met het oog op het algemeen belang.
24 okt 2023	Hackers die eind 2022 digitaal inbraken bij de gemeente Asten hadden toegang tot de persoonlijke gegevens van 612 personen uit de gemeente. Dat bleek uit onderzoek. Zij kregen allemaal een brief van de gemeente. De digitale inbrekers kwamen in de computers van ambtenaren via factuurfraude. De dieven stuurden een nepfactuur met daarop een onbekend bedrag dat de gemeente moest betalen. De ambtenaren vertrouwden het niet en maakten het geldbedrag niet over, maar er werd wel op de link geklikt. Daardoor kregen de hackers toegang tot twee mailboxen met daarin 23.000 bestanden en andere gegevens.
16 nov 2023	Regering raadt het gebruik van AI-software door rijksambtenaren af. ‘Niet gecontracteerde generatieve AI-toepassingen voldoen over het algemeen niet aantoonbaar aan de Nederlandse privacy- en auteursrechtelijke wetgeving’
17 nov 2023	De Autoriteit Persoonsgegevens (AP) legt de gemeente Voorschoten een boete op van 30.000 euro. De reden is dat de gemeente informatie over afval van individuele huishoudens veel langer bewaarde dan nodig was.
8 dec 2023	De EU-landen en het Europees Parlement hebben een voorlopig akkoord bereikt over regels voor AI (AI-act).
21 dec 2023	Publicatie AP jaarplan 2024. In 2024 besteedt de AP extra aandacht aan deze vijf thema’s: Algoritmes & AI, Big Tech, Vrijheid & Veiligheid, Datahandel, Digitale Overheid.

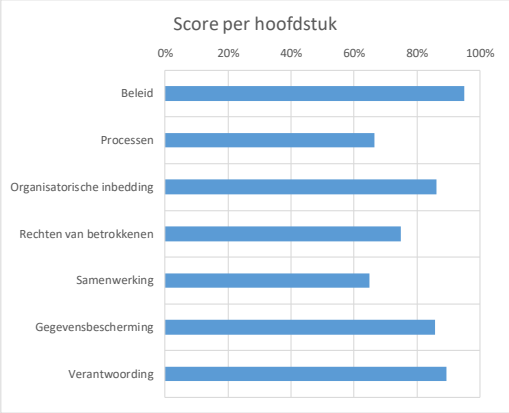
Bijlage 4 Overzicht AVG borgingsproduct 3.0

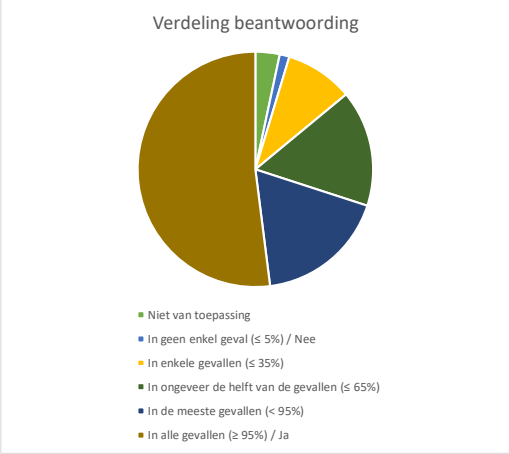
Borgingsproduct AVG v3.0
Dashboard

INFORMATIE BEVEILIGINGS DIENST

Naam organisatie	Gemeente Deurne
Datum ingevuld	4 januari 2024
Aantal beantwoord	145 van de 155
Score	78%

Par	Titel	Leeg	N.v.t	Beantwoord	Percentage
1.	Beleid	0	2	15	95%
1.1	Beleid vaststellen	0	0	2	100%
1.2	Privacybeleid	0	2	7	96%
1.3	Verantwoordelijkheden	0	0	6	92%
2.	Processen	0	0	38	66%
2.1	Werkprocessen	0	0	7	50%
2.2	Verwerkingsregister	0	0	10	75%
2.3	Pre-DPIA's	0	0	3	67%
2.4	DPIA's	0	0	10	85%
2.5	Bewaar- en vernietigingsbeleid	0	0	8	47%
3.	Organisatorische inbedding	0	0	20	86%
3.1	Privacyteam	0	0	2	88%
3.2	Aanstelling, positie en taken FG	0	0	11	86%
3.3	Informeren OR	0	0	2	88%
3.4	Bewustwording	0	0	5	85%
4.	Rechten van betrokkenen	0	3	27	75%
4.1	Recht op informatie	0	0	5	80%
4.2	Processen rechten van betrokkenen	0	0	9	89%
4.3	Toestemming	0	0	4	63%
4.4	Geautomatiseerde individuele besluitvorming	0	3	2	75%
4.5	Websites en applicaties	0	0	3	75%
4.6	Technische ondersteuning	0	0	4	50%
5.	Samenwerking	5	0	10	65%
5.1	AVG rollen	0	0	8	66%
5.2	Gegevensverstrekking	5	0	2	63%
6.	Gegevensbescherming	0	0	28	86%
6.1	Risico's	0	0	2	100%
6.2	Gegevensbescherming door ontwerp	0	0	2	88%
6.3	Gegevensbescherming door standaardinstellingen	0	0	1	50%
6.4	Informatiebeveiliging	0	0	10	78%
6.5	Privacyincidenten en datalekken	0	0	13	92%
7.	Verantwoording	0	0	7	89%
7.1	Evaluatie naleving AVG	0	0	4	81%
7.2	Evaluatie informatiebeveiliging	0	0	2	100%
7.3	Rapportage	0	0	1	100%





FG analyse

In 2023 werd intern gebruik gemaakt van het AVG Borgingsproduct 3.0 van de Vereniging Nederlandse Gemeenten (VNG) als hulpmiddel om meer inzicht te krijgen in hoeverre de gemeente in staat is om de naleving van de AVG te waarborgen. Uit het bovenstaande overzicht blijkt dat er de afgelopen jaren goede stappen zijn gemaakt in opzet en bestaan van beheersmaatregelen.