

VERTROUWELIJK

gemeente Eindhoven
Bureau Functionaris Gegevensbescherming
[REDACTED]
Januari 2020

**

Detail bedrijfsinformatie AVG 2019

Inhoud

- I. Verwerkingsregister
- II. Data Protection Impact Assessments
- III Datalekken
- IV Rechten van betrokkenen
- V Klachten
- VI Privacyplannen sectoren
- VII Vergelijking met andere gemeenten
- VIII Conclusies en aanbevelingen



I. Verwerkingsregister.

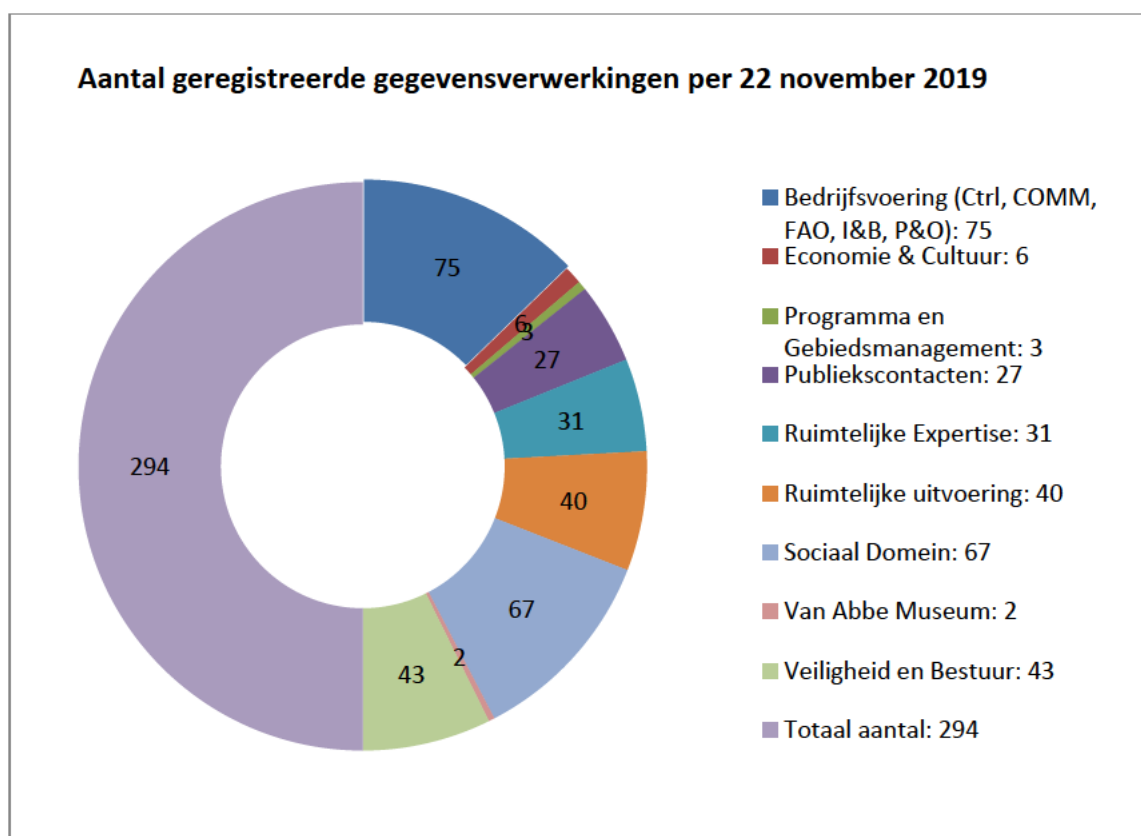
De AVG verplicht tot het opnemen van alle verwerkingen in een register, dat continu actueel moet worden gehouden. Op basis van het privacybeleid van de gemeente zijn sectoren hiervoor verantwoordelijk en is het beheer van het register neergelegd bij bureau FG.

Tot 2019 werd een excelbestand voor dit register gebruikt. In 2019 vond een kwaliteitsslag plaats, waarbij gebruik is gemaakt van geautomatiseerde ondersteuning, namelijk de applicatie "SmartPia" van het bedrijf Usoft.

Aan sectoren¹ is gevraagd alle verwerkingen voor eind 2019² te registreren in SmartPia. Eind 2019 is geconstateerd dat nog niet alle verwerkingen (volledig) waren opgenomen in SmartPia. Dit is risicovol omdat de gemeente daarmee niet beschikt over een volledig en actueel register, zoals voorgeschreven in de AVG. Aan sectoren is daarom gevraagd de verwerkingen alsnog op te nemen in SmartPia, voor 1 mei 2020.

Verwerkingen die niet zijn opgenomen in SmartPia kunnen als niet rechtmatig worden aangemerkt.

Onderstaand schema geeft een beeld per sector³:



¹ De privacy officers van de sectoren.

² 2019 is in dat opzicht een overgangsjaar geweest.

³ Sectoren die niet in het overzicht zijn opgenomen, hebben geen verwerkingen geregistreerd.



Gegevensverwerkingen worden in SmartPia geregistreerd door het invullen van een zogenoemde "quicksan". Dit is een digitaal formulier. De hierin opgenomen vragen zijn gebaseerd op de eisen die de AVG aan een registratie stelt. Deze quickscans worden door bureau FG beoordeeld en geclassificeerd op risico-gevoeligheid⁴. Op basis van deze classificatie wordt aan sectoren geadviseerd een Data Protection Impact Assessment (DPIA) te starten. Voor bestaande risicovolle verwerkingen geldt hiervoor een termijn van mei 2021. Naast rechtmatigheid is dit de reden dat aan sectoren is gevraagd voor mei 2020 alle verwerkingen (alsnog) op te nemen in SmartPia. Op deze manier heeft een sector tijdig inzicht in het aantal uit te voeren DPIA's. Zodat deze tijdig kunnen worden ingepland.

II. Data Protection Impact Assessments (DPIA's)

De AVG verplicht de gemeente DPIA's uit te voeren bij verwerkingen met een hoog privacy risico. Een DPIA is een feitelijke risico inventarisatie waar maatregelen tegenover worden gesteld. De AVG geeft strikt aan waar een DPIA aan moet voldoen. Een uitgevoerde DPIA moet minimaal eens per drie jaar worden herhaald. Het beeld per sector ziet er voor 2019 als volgt uit.

	SD	Ctrl	P&O	I&B	VB	Pu-Co	PGM	RE	RU	Totaal
Aantal lopende DPIA's per 1-1-2019	8	0	0	1	1	0	0	0	1	11
Aantal in 2019 gestarte DPIA's	9	1	1	0	4	3	1	5	0	24
Aantal in 2019 afgeronde DPIA's	9 ⁵	0	0	1	1	2	0	2	1	16
Aantal lopende DPIA's per 31-12-2019	8	1	1	0	4	1	1	3	0	19

⁴ Op basis van criteria uit de AVG en van de Autoriteit Persoonsgegevens.

⁵ Van de 9 afgeronde DPIA's is 1 DPIA door de sector ingetrokken.



Sectoren die in dit overzicht niet voorkomen betreffen sectoren die:

- geen (risicovolle) verwerkingen hebben ingediend; of
- bestaande risicovolle verwerkingen uitvoeren maar die nog geen DPIA hebben ingepland. Deze DPIA's zouden voor mei 2021 moeten worden uitgevoerd ⁶.

Doorlooptijd afgeronde DPIA's.

Het uitvoeren van een DPIA kost tijd. Binnen de gemeente Eindhoven geldt als stelregel dat een DPIA binnen 6 weken moet worden afgerond. Deze termijn wordt op dit moment niet gehaald. In onderstaande tabel is, per sector, de gemiddelde doorlooptijd van een DPIA opgenomen. Dit betreft de DPIA's die in 2019 zijn afgerond.

	SD	I&B	VB	Pu-Co	RE	RU
Gemiddelde doorlooptijd afgeronde DPIA's in 2019	9,4 maanden	14 maanden	9 maanden	2,5 maanden	4 maanden	12 maanden

DPIA's, en de implementatie van de daaruit voortvloeiende maatregelen, moeten zijn afgerond voordat de (gewijzigde) verwerking start. Dit is een harde eis die voortkomt uit de AVG. Bij een tweetal uitgevoerde DPIA's is geconstateerd dat de verwerking is gestart zonder dat de uit de DPIA voortgekomen maatregelen waren geïmplementeerd. Dit maakt deze verwerkingen onrechtmatig in de zin van de AVG. Bij 1 sector zijn risicovolle verwerkingen gewijzigd, zonder dat de vereiste DPIA's waren uitgevoerd. Ook dat maakt de verwerkingen onrechtmatig in de zin van de AVG.

Dit is risicovol voor de gemeente omdat niet aantoonbaar is geborgd dat tijdig adequate maatregelen zijn getroffen om risico's weg te nemen bij deze verwerking. Het gaat dan niet alleen om privacy risico's maar ook om risico's op gebied van informatieveiligheid. Het verwerkersverantwoordelijke management is gewezen op de risico's.

Bij sectoren die inmiddels meerdere DPIA's hebben uitgevoerd, is overigens te zien dat de kwaliteit van de DPIA's verbeterd.

Nog uit te voeren DPIA's voor bestaande verwerkingen.

Niet alleen voor nieuwe verwerkingen moeten tijdig DPIA's worden uitgevoerd. Ook voor bestaande verwerkingen⁷ met een hoog risico profiel geldt dat een DPIA noodzakelijk is. Hiervoor geldt in principe⁸ de termijn van mei 2021.

⁶ Tenzij de risicovolle verwerkingen wijzigen of nieuwe risicovolle verwerkingen worden gestart: dan is een DPIA noodzakelijk voordat de (gewijzigde) verwerking start.

⁷ Een bestaande verwerking is een verwerking die in mei 2018 al liep.

⁸ Indien de verwerking wijzigt, zal in de meeste gevallen eerder een DPIA vereist zijn. Namelijk voordat de gewijzigde verwerking start.



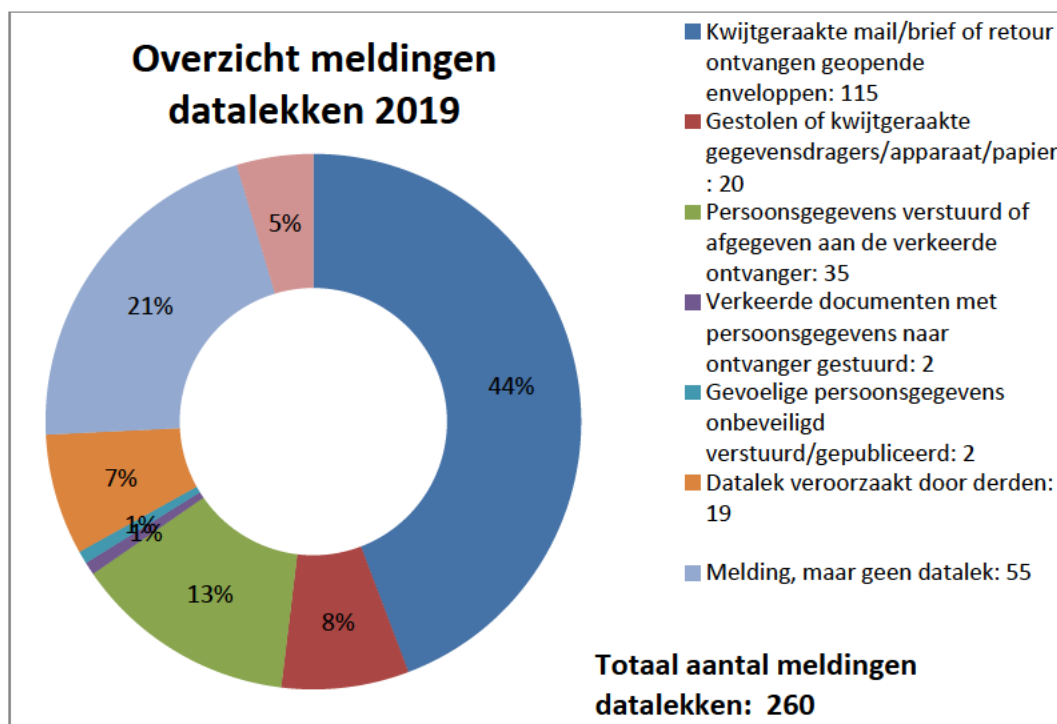
Op basis van de verwerkingen ("quick scan") die sectoren hebben ingediend voor het verwerkingsregister is nu het beeld dat het daarbij gaat om de navolgende aantallen, uit te voeren DPIA's voor mei 2021:

FAO	2
EC	1
SD	23
I&B	3
VB	14
PuCo	13
RE	1

Voor sectoren die hier niet worden genoemd, geldt dat op dit moment geen bestaande verwerkingen zijn ingediend waarvoor DPIA's noodzakelijk zijn.

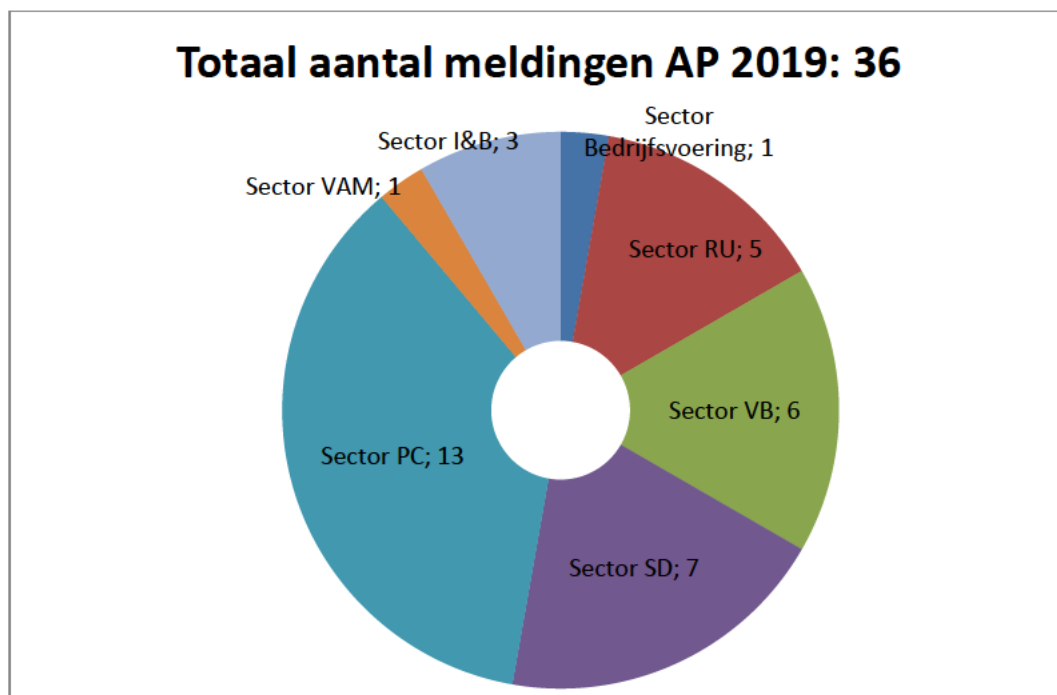
Bij dit overzicht geldt nadrukkelijk de kanttekening dat dit een momentopname is, omdat een aanzienlijk aantal verwerkingen nog niet volledig door sectoren zijn ingediend. Deze verwerkingen zijn nog niet beoordeeld op de vraag of een DPIA noodzakelijk is. Dit geldt eveneens voor verwerkingen die zijn ingediend, maar waar nog vragen of opmerkingen bij waren. Ook dit betreft een significant aantal.

III. Datalekken





Totaal aantal bij de AP gemelde datalekken per sector:



IV. Rechten van betrokkenen.

In 2019 werd 29 keer een beroep gedaan op de "rechten van betrokkenen". Dit betreft bijvoorbeeld een verzoek om inzage van de verwerkte gegevens of een verzoek om correctie of verwijdering van verwerkte gegevens.

Sector Personeel en Organisatie heeft 3 verzoeken behandeld. Bij Sociaal Domein ging het om 14 verzoeken. Publiekscontacten heeft 7 verzoeken behandeld. Ruimtelijke Expertise heeft 2 verzoeken behandeld. Veiligheid, Juridische Zaken en Bestuur heeft 3 verzoeken behandeld.

V. Klachten

Personen die in de knel komen door verkeerde gegevensverwerking of die zich benadeeld voelen door een verwerking, hebben wettelijk recht op toegang tot de FG. De FG heeft in deze gevallen een ombudsfunctie en toetst of de gegevensverwerking rechtmatig, doelmatig, betrouwbaar en veilig is geweest.



In 2019 werden 10 klachten ingediend bij FG. Een specificatie levert het navolgende beeld op:

	PuCo	SD	VB	PGM	RU
Ongegrond	4				
Gegrond		1	1	1	
Ingetrokken		1			
Niet van toepassing op de gemeente Eindhoven					1
Niet in behandeling genomen			1		

VI. Privacyplannen

Het privacybeleid van de gemeente Eindhoven van mei 2018 schrijft voor dat iedere sector privacy plannen opstelt. Doel is vooral het stimuleren van privacy-bewustzijn bij medewerkers en het sturen op naleven van regels door medewerkers en gedrag van medewerkers. Ook het treffen van compliance maatregelen is een doelstelling van een dergelijk plan. Een sector privacy plan is ook cruciaal in het aantoonbaar komen tot een PDCA-cyclus (Plan, Do, Check & Act), zoals opgenomen in het privacybeleid van de gemeente. Een actieve PDCA cyclus is cruciaal voor het aantoonbaar naleven van de AVG door de organisatie.

Per 31 december 2019 hadden 4 van de 14 sectoren een plan opgesteld. Het gaat om de sectoren: Sociaal Domein, Veiligheid, Juridische Zaken en Bestuur, Ruimtelijke Uitvoering en Facilitaire & Administratieve Ondersteuning. Dit beeld is zorgwekkend. Het overgrote deel van de sectoren binnen de gemeente hebben op dit onderdeel geen uitvoering gegeven aan het privacybeleid.

VII. Conclusie, zorgpunten en aanbevelingen.

Zorgvuldig omgaan met persoonsgegevens is een continu proces en vraagt blijvende inzet van zowel bestuur, management als medewerkers.

Hiervoor is allereerst nodig dat AVG-verplichtingen structureel de aandacht hebben van de sectoren. Om toe te groeien naar een volwassenheidsniveau, waar de AVG van uit gaat, is (extra) inzet van de organisatie nodig. Dit gaat allereerst om het feitelijk invullen van de verantwoordelijkheden, zoals vastgelegd in het privacybeleid van de gemeente. Bij de inrichting van werkprocessen zal al in een vroeg stadium aandacht moeten zijn voor privacy, om een zorgvuldige omgang met persoonsgegevens van begin af aan borgen. Ook de toepassing van gerichte juridische kwaliteitszorg en / of juridische control door de organisatie, is een cruciale factor bij de verdere borging van de AVG in de werkprocessen. Verder zal de organisatie het verwerkingsregister voortdurend actueel moeten houden, zullen er tijdig DPIA's moeten worden uitgevoerd en moeten datalekken altijd worden gemeld.

De AVG heeft een blijvende grote invloed op bijna alle processen van de gemeente en daarmee ook op het werk van de sectoren. Er is in 2019 (en 2018) een basis gelegd. Het



is zaak om daar de komende jaren met volle energie op voort te bouwen. Want er ligt nog een grote opgave. De AVG blijft structurele inzet van de organisatie vragen.

Zorgpunt op dit moment is onder meer de volledigheid en de actualiteit van het verwerkingsregister. Ook het aantal uitgevoerde DPIA's is nog erg beperkt in relatie tot het aantal risicovolle verwerkingen. Daarnaast baart de lange doorlooptijd van de uitgevoerde DPIA's zorgen: advies is voldoende tijd en capaciteit beschikbaar te stellen om de DPIA's binnen een redelijke termijn (6 weken) af te ronden. Specifiek voor de sector Veiligheid, Juridische Zaken en Bestuur geldt dat hier bij uitstek veel verwerkingen voorkomen die zeer risicovol zijn. Het aantal afgeronde DPIA's bij deze sector is nog minimaal in verhouding tot het aantal risicovolle verwerkingen. Aanbeveling voor deze sector is dan ook om in 2020 een inhaalslag te maken.

Tenslotte is onderdeel bedrijfsvoering kwetsbaar gebleken als het gaat om het voldoen aan de AVG. De acceptatiegraad bij het volgen van de AVG-spelregels is bij een aantal van de bedrijfsvoeringsectoren laag. Er is weerstand bijvoorbeeld bij registratie van datalekken, het tijdig nemen van maatregelen om datalekken te voorkomen en te beëindigen. DPIA's worden niet op tijd uitgevoerd (voor start van de verwerking) of worden wel uitgevoerd, maar de daaruit volgende maatregelen worden niet tijdig geïmplementeerd.

De top 5 van praktische / operationele aanbevelingen voor de sectoren zijn:

1. Kom zo snel mogelijk alsnog tot een sector privacy plan, op basis van het privacy beleid 2018. Richt op basis van dit privacy plan een PDCA-cyclus in, zoals opgenomen in het privacy beleid 2018.
2. Geef (bijvoorbeeld) in afdelings- en sectoroverleggen continu aandacht aan de verwerking van persoonsgegevens en het aantoonbaar voldoen aan de regelgeving. Besteed ook op MT-niveau continu aandacht aan dit thema.
3. Het aantal datalekken is teruggelopen (in tegenstelling tot de landelijke trend). Moedig het melden van datalekken aan. Besteed hier aandacht aan tijdens werkoverleggen. Wijs medewerkers er op dat datalekken onmiddellijk gemeld moeten worden via meldpuntdatalekken@eindhoven.nl (in ieder geval binnen 24 uur na ontdekking). Dus niet wachten tot na het weekend, ook in het weekend en 's avonds worden datalekken in behandeling genomen; dit laatste is van belang wanneer het gaat om verlies van een telefoon, surface of laptop!
4. Toets regelmatig of gebruikte persoonsgegevens actueel en juist zijn en neem dit op in de PDCA-cyclus.
5. Kom zo snel mogelijk tot een volledig verwerkingsregister en maak op basis daarvan een planning voor het –voor mei 2021- uitvoeren van DPIA's. Voer tijdig een DPIA's uit bij wijziging van een bestaande verwerking of bij een nieuwe verwerking (voordat de verwerking start). Pas "privacy by design" toe: dat wil zeggen betrek de AVG in een vroeg stadium bij de ontwikkeling van producten of diensten.

En tot slot: schakel op tijd bureau FG in. En maak gebruik van de expertise, ervaring en adviezen van dit bureau.