Gemeente Deurne

Rapportage informatiebeveiliging 2021

op basis van ENSIA

Leeswijzer en inhoud

Deze rapportage is opgesteld op basis van de zelfevaluatie ENSIA 2021

TERUGBLIK 2021
- Ontwikkelingen
- Resultaat bij belangrijkste doelen
- Beveiligingsincidenten en datalekken

STATUS INFORMATIEBEVEILIGING (BIO)
- Onze norm voor informatiebeveiliging samengevat (de BIO)
- Status Deurne ten opzichte van de BIO

VERANTWOORDING AAN HET RIJK
- Getoetste collegeverklaring ENSIA – DigiD
- Getoetste collegeverklaring ENSIA – Suwinet
- Status Basisregistratie Personen en Reisdocumenten
- Status GEO basisregistraties (BAG, BGT, BRO)

De BIO maatregelen zijn in deze rapportage beknopt opgenomen.

GEBRUIKTE SCHALEN:

groen: goed (90% - 100% van de punten)
oranje: voldoende (75% - 90% van de punten)
rood: onvoldoende (0% - 75% van de punten)

groen: voldaan aan een norm
rood: niet voldaan aan een norm

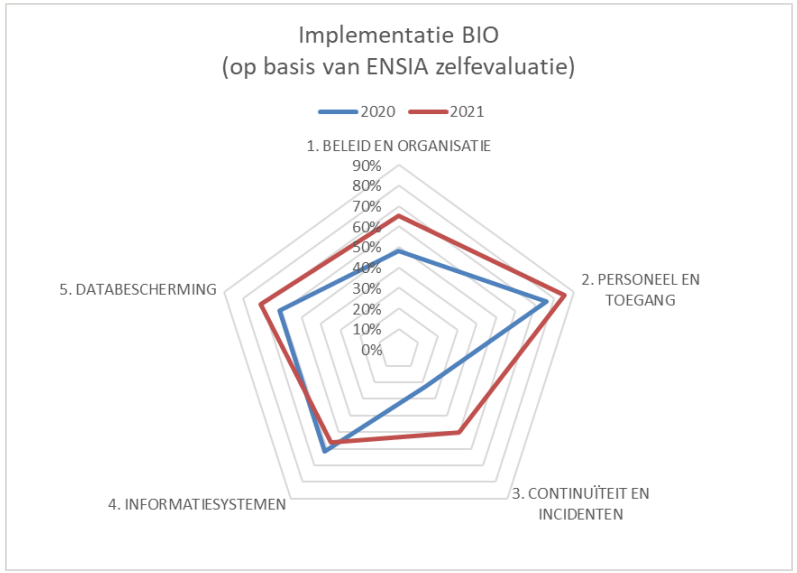
TERUGBLIK 2021

Belangrijke ontwikkelingen in 2021

Deurne

- Nieuw beleid voor informatiebeveiliging maakt rollen en verantwoordelijkheden helder.
- Management stuurt stevig op e-Learning rond privacy & informatiebeveiliging. Bewustzijn en bereidheid om maatregelen te nemen groeien.
- Gemeenteraad kent middelen toe om de basis op orde te brengen in onze informatievoorziening.

- Implementatie BIO van groeit naar 68% (was 60%)



Nederland en de wereld

- Wet Open Overheid (1 mei 2022) vergt extra aandacht voor informatieclassificatie en -beveiliging in processen en systemen.
- Oligopolies: toenemende afhankelijkheid van dominante commerciële partijen.
- Thuiswerken blijft bestaan. Focus moet verschuiven van beveiliging van een gesloten netwerk naar beveiliging van applicaties en data thuis en in een open omgeving.
- Meer gebruik van SaaS-applicaties zorgt voor risicospreiding maar vraagt ook om versterking van regie om zicht te houden op risico's.
- Ransomware ontwikkelt zich verder waardoor de kans op incidenten hoog blijft.
- Toenemende tekorten op de arbeidsmarkt van cybersecurity- en ICT specialisten.
- Oproep VNG voorzitter aan alle burgemeesters om organisatie digitaal weerbaar te maken. Belang onderstreept door Log4J bijna-crisis.

Resultaten 2021

- Capaciteitsgebrek op informatisering, automatisering, privacy en security belemmert voortgang.
- Steeds volwassener op IB & P. Leiding en medewerkers pakken integrale verantwoordelijkheid goed op.
- Vruchtbare samenwerking en kennisuitwisseling in de regio.

Risico	Resultaten	Oordeel
2	Een nieuw informatiebeveiligingsbeleid met uitwerking van rollen, verantwoordelijkheden en wettelijke eisen is vastgesteld.	goed
3	Inkoopeisen voor ICT in gebruik genomen, privacy en informatiebeveiliging zijn hiervan een onderdeel. IB & P in 2022 bij elke inkoopstrategie.	goed
13	Accounts met bijzondere (beheer-) rechten worden regelmatig beoordeeld.	goed
22	Respons op een groot (dreigend) beveiligingsincident werd geoefend en geevalueerd tijdens de landelijke crisis rond Log4j2.	goed
24	Informatiebeveiliging opgenomen in de interne controles van P&O processen.	goed
27	Met afdeling Samenleving zijn acties geformuleerd om privacy verder in te bedden.	goed
29	Deurne voldoet aan de norm NTA 7516 voor veilig berichtenverkeer.	goed
33	Informatiebeveiliging is integraal onderdeel van alle P&O procedures.	goed
44	Beleid voor beveiliging van ruimtes en gebouwen werd vastgesteld.	goed
45	Sleutelplannen voor externe locaties opgesteld.	goed
46	Procedures rond kluis burgerzaken aangescherpt.	goed
61	Geen grote risico's gevonden bij specialistisch onderzoek naar technische kwestbaarheden (penetratietest).	goed
22	Back-up voor het zaaksysteem en Office 365 is geïmplementeerd. Herstelplan voor de volledige keten volgt in 2022.	voldoende
1	Invoering van een P&C cyclus voor informatiebeveiliging is 2021 goed gevorderd. Risicomanagement en interne controles nog niet goed ontwikkeld.	voldoende
5	Voor 20 belangrijke applicaties zijn enkele informatiebeveiligingsrichtlijnen specifiek getoetst.	voldoende
12	Projectvoorstel en business case opgesteld voor een SIEM/SOC. Besluitvorming en uitvoering in 2022.	voldoende
50,51	Vernieuwde netwerkinfrastrustuur biedt meer veiligheid. Verder inrichten is nodig.	voldoende
4	Opzet van de kernregistratie processen en gegevensverwerkingen (verwerkingsregister) is nog niet gestart.	onvoldoende
9	Geen voortgang in het beleggen en verbeteren van contractbeheer.	onvoldoende
14,36,37	Implementatie van beleid logische toegangsbeveiliging verloopt moeizaam. Periodieke controle toegangsrechten en opvolgen afwijkingen niet geborgd.	onvoldoende
17	Beheer van applicaties en data op mobiele apparaten (MAM) nog niet verbeterd.	onvoldoende
28,38	Toegangsbeveiliging (autorisaties) in het zaaksysteem kon niet worden verbeterd.	onvoldoende
32	Beveiliging van mobiele aparatuur niet geborgd met controles.	onvoldoende
56,58	Weinig controle op naleven van privacybeleid.	onvoldoende

Informatiebeveiligingsincidenten en Datalekken

	2018	2019	2020	2021
Beveiligingsincidenten	onbekend	onbekend	23	27
waarbij persoonsgegevens betrokken (datalek)	8	10	14	13
gemeld aan autoriteit persoonsgegevens	3	5	4	4
gemeld aan of door betrokkenen	0	0	4	6

* Toename wijst op betere registratie, niet noodzakelijk op meer incidenten en datalekken.

STATUS INFORMATIEBEVEILIGING

op basis van de Baseline
Informatiebeveiliging Overheid (BIO)

DE BASELINE INFORMATIEBEVEILIGING OVERHEID (BIO)

Alle gemeentes volgen de BIO. Dit zijn verplichte maatregelen voor informatiebeveiliging.
Ze kunnen in 5 groepen worden samengevat.

BIO Hoofdstuk		Normen	Consolidatie	Totaal	
5	Informatiebeveiligingsbeleid	2	1. BELEID EN ORGANISATIE	23	181
6	Organiseren van informatiebeveiliging	11			
18	Naleving	10			
7	Veilig personeel	7	2. PERSONEEL EN TOEGANG	54	
9	Toegangsbeveiliging	27			
11	Fysieke beveiliging en beveiliging van de omgeving	20			
16	Beveiligingsincidenten (Beheer van informatie..)	13	3. CONTINUÏTEIT EN INCIDENTEN	18	
17	Bedrijfscontinuïteitsbeheer (Informatiebeveiligingsaspecten van ..)	5			
12	Beveiliging bedrijfsvoering	30	4. INFORMATIESYSTEMEN	55	
14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	13			
15	Leveranciersrelaties	12			
8	Beheer van bedrijfsmiddelen	14	5. DATABESCHERMING	31	
10	Cryptografie	4			
13	Communicatiebeveiliging	13			

SAMENGEVAT: WAT SCHRIJFT DE BIO VOOR

Bestuurlijke principes en beleid, organisatie van de beveiliging en naleving

Het bestuur van Deurne:

- Volgt het beleid van de informatiebeveiligingsdienst gemeenten (IBD)
- Zorgt ervoor dat de juiste activiteiten voor informatiebeveiliging door de organisatie worden uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

1. BELEID EN ORGANISATIE
H5 / H6 / H18

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

- Bestuur, directie en management laten zien dat informatiebeveiliging belangrijk is
- Informatiebeveiliging is georganiseerd
- Wij houden ons aan onze afspraken en leven de wet- en regelgeving na

Het bestuur en medewerkers zijn actief betrokken bij informatiebeveiliging. Er is een organisatiebreed beleid dat richting en sturing geeft. De organisatie is effectief ingericht, waarbij rollen, taken en bevoegdheden zijn ondergebracht. Verantwoording is structureel ingericht, zodat naleving is geborgd.

2. PERSONEEL EN TOEGANG
H7 / H9 / H11

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

- Voor, tijdens en na het dienstverband is alles goed geregeld
- Medewerkers gaan bewust om met informatie
- Medewerkers hebben juiste toegangsrechten (fysiek en digitaal)

Alleen de juiste personen hebben toegang tot de gebouwen, systemen en gegevens van de gemeente. Er zijn passende maatregelen, zowel in organisatie als in techniek. Dit gaat om waarborgen rondom in- en externe medewerkers, toegang tot gebouwen en omgeving en toegang tot de (digitale) informatievoorziening.

SAMENGEVAT: WAT SCHRIJFT DE BIO VOOR

3. CONTINUÏTEIT EN INCIDENTEN
H16 / H17

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten

- Wij komen afspraken met inwoners na
- Bij calamiteiten en incidenten weten we wat we moeten doen
- Continuïteitsplannen zijn actueel en worden getest
- Incidenten worden altijd gemeld

De diensten van de gemeente worden geleverd volgens de afspraken die de gemeente daarover maakt met inwoners en bedrijven. Ook bij incidenten worden de diensten geleverd volgens deze afspraken.

4. INFORMATIESYSTEMEN
H12 / H14 / H15

Veilige omgang met informatiesystemen en afspraken hierover met leveranciers

- Wijzigingen in systemen worden op een gecontroleerde manier doorgevoerd
- We zijn beschermd tegen malware
- Back-ups worden volgens beleid uitgevoerd en getest
- De afspraken met leveranciers zijn vastgelegd

Informatiesystemen zijn een keten van mensen, processen en middelen. Hierin zijn procedures en maatregelen beschikbaar ter bescherming van de omgeving. Het gaat hierbij om zowel de interne als de externe informatiesystemen (uitbesteding, leveranciers en Cloud- toepassingen).

5. DATABESCHERMING
H8 / H10 / H13

Veilige omgang met data in applicaties

- Data wordt op de juiste manier beschermd
- De gegevens van de burgers worden veilig opgeslagen en gecommuniceerd. Binnen en buiten de gemeente

STATUS DEURNE TEN OPZICHT VAN DE BIO

Goede vooruitgang in werken volgens de BIO.
Op belangrijke punten wordt nog niet aan de norm voldaan. Hierdoor lopen we risico's.
De focus moet uitgaan naar:

- verder invoeren en borgen toegangsbeveiliging
- testen van wijzigingen in informatiesystemen
- monitoring en detectie van incidenten (SIEM/SOC)
- back-up en herstel in ketens van applicaties
- voorbereiden op grote incidenten (cybercrisis, continuïteitsplan)

onvoldoende

68%

0% - 75% 75% - 90% 90% - 100%

1. BELEID EN ORGANISATIE Actueel beleid en organisatie van informatiebeveiliging en controle op naleving	65%
2. PERSONEEL EN TOEGANG Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens	85%
3. CONTINUÏTEIT EN INCIDENTEN Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten	50%
4. INFORMATIESYSTEMEN Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers	56%
5. DATABESCHERMING Veilige omgang met data in onze software	71%

1. BELEID EN ORGANISATIE

Onvoldoende

65%

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

- Bestuur, directie en management laten zien dat informatiebeveiliging belangrijk is
- Informatiebeveiliging is georganiseerd
- Wij houden ons aan onze afspraken en leven de wet- en regelgeving na

Onderdelen:

0% - 75% | 75% - 90% | 90% - 100%

H5 / Informatiebeveiligingsbeleid	100%
H6 / Organiseren van informatiebeveiliging	64%
H18 / Naleving	60%

Bevindingen en verbeteracties

- *Vaststellen eisen aan beveiligingsniveau (BBN) door verantwoordelijke voor een proces*
- *Overzicht contacten en beveiligingseisen (overheids-)instanties en toezichthouders*
- *Planmatig uitvoeren audits op informatiebeveiliging*
- *Regelmatige controles op naleven privacy regels, procedures en verwerking persoonsgegevens*

Risico's

- *Procesverantwoordelijke neemt geen eigenaarschap voor informatiebeveiliging*
- *In- en externe wet- en regelgeving privacy & informatiebeveiliging worden niet nagekomen*
- *Geen zicht op naleving, daardoor niet in control en onbekende risico's*

2. PERSONEEL EN TOEGANG

voldoende

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

- Voor, tijdens en na het dienstverband is alles goed geregeld
- Medewerkers gaan bewust om met informatie
- Medewerkers hebben juiste toegangsrechten (fysiek en digitaal)

85%

Onderdelen:

0% - 75% | 75% - 90% | 90% - 100%

H7 / Veilig personeel	100%
H9 / Toegangsbeveiliging	78%
H11 / Fysieke beveiliging en beveiliging van de omgeving	90%

Bevindingen en verbeteracties

- *Beleid voor toegang tot informatiesystemen invoeren en borgen met controles*
- *Breder beschikbaar stellen wachtwoordkluis*
- *Verder invoeren en borgen beleid voor fysieke toegangsbeveiliging*

Risico's

- *Vertrouwelijke informatie en persoonsgegevens zijn in te zien door medewerkers die dit niet nodig hebben*
- *Wachtwoorden zijn zwak en/of worden hergebruikt in meerdere systemen*
- *Toegang tot locaties en gebouwen onvoldoende beschermd*

3. CONTINUÏTEIT EN INCIDENTEN

onvoldoende

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten

- Wij komen afspraken met inwoners na
- Bij calamiteiten en incidenten weten we wat we moeten doen
- Continuïteitsplannen zijn actueel en worden getest
- Incidenten worden altijd gemeld

50%

Onderdelen:

0% - 75% | 75% - 90% | 90% - 100%

H16 / Beheer van beveiligingsincidenten	69%
H17 / Bedrijfscontinuïteitsbeheer & informatiebeveiliging	0%

Bevindingen en verbeteracties

- *Opstellen en oefenen van een responsplan voor beveiligingsincidenten en calamiteiten (cybercrisisplan)*
- *Contracteren expertise voor bijstand bij cyberincidenten en/of sluiten cyberrisicoverzekering*
- *Bedrijfscontinuïteitsplannen om dienstverlening overeind te houden tijdens een calamiteit*

Risico's

- *Bij onjuist reageren groeit een incident uit tot calamiteit met politieke, maatschappelijke en financiële schade.*
- *De dienstverlening aan inwoners komt na een ernstig incident of gerichte cyber-aanval langdurig stil te liggen.*

4. INFORMATIESYSTEMEN

onvoldoende

56%

Veilige omgang met informatiesystemen en afspraken hierover met leveranciers

- Wijzigingen in systemen worden op een gecontroleerde manier doorgevoerd
- We zijn beschermd tegen malware
- Back-ups worden volgens beleid uitgevoerd en getest
- De afspraken met leveranciers zijn vastgelegd

Onderdelen: 0% - 75% | 75% - 90% | 90% - 100%

H12 / Beveiliging van de bedrijfsvoering	40%
H14 / Acquisitie, ontwikkeling en onderhoud van informatie systemen	77%
H15 / Leveranciersrelaties	75%

Bevindingen en verbeteracties

- *Back-ups maken, testen en beschermen op een manier die past bij het belang van de informatie*
- *Testen van nieuwe en aangepaste applicaties gecontroleerd en (liefst) zonder persoonsgegevens buiten productie*
- *Expliciete risicoafweging bij bepalen beveiligingseisen en aangaan contracten met leveranciers*
- *Beter contractbeheer en controle op naleven van afspraken door leveranciers en partners*
- *Logs van gebeurtenissen op systemen (automatisch) controleren om cyberdreigingen te kunnen opmerken (GGI-Veilig: SIEM/SOC)*

Risico's

- *Informatie die niet goed geback-upt is gaat verloren door een ongeluk of cyber-aanval*
- *De dienstverlening wordt verstoord door niet opgemerkte fouten in een nieuwe of aangepaste applicatie*
- *Persoonsgegevens worden onrechtmatig verwerkt bij het testen van applicaties*
- *Risico's voor informatiebeveiliging bij uitbesteden of samenwerken worden niet beheerst*
- *Hackers zijn al binnen zonder dat het wordt opgemerkt. Gevolg: dienstverlening ligt weken stil (zie Hof van Twente)*

5. DATABESCHERMING

voldoende

71%

Veilige omgang met data in onze applicaties
- Data wordt op de juiste manier beschermd
- De gegevens van de burgers worden veilig opgeslagen en gecommuniceerd.
- Binnen en buiten de gemeente

Onderdelen:

0% - 75% 75% - 90% 90% - 100%

H8 / Beheer van bedrijfsmiddelen	79%
H10 / Cryptografie	0%
H13 / Communicatiebeveiliging	85%

Bevindingen en verbeteracties
- *Informatie passend beveiligen en beschermen door het eerst te classificeren zodat eisen en risico's duidelijk worden*
- *Beleid en regie op gebruik van versleuteling om gegevens te beschermen*
- *Technisch beter beschermen van (gemeentelijke) informatie bij thuis- en mobiel werken*
- *Computernetwerk van het gemeentehuis veiliger inrichten met afgescheiden "kamers" (segmenten)*

Risico's
- *Informatie wordt niet juist beveiligd en beschermd met politieke, organisatie- of persoonlijke schade als gevolg*
- *Informatie wordt onveilig en/of onrechtmatig verwerkt op mobiele apparaten die ook privé eigendom kunnen zijn*
- *Een aanvaller (cyber-crimineel) die in ons netwerk binnen is kan ongehinderd alle "kamers" doorzoeken*

ENSIA VERANTWOORDING AAN HET RIJK

Getoetste collegeverklaring ENSIA - DIGID

voldaan

Van onze ENSIA-zelfevaluatie worden jaarlijks twee onderdelen geaudit door een IT-auditor: DigiD en Suwinet. De basis voor de audit vormt de collegeverklaring. Hierin zijn de uitkomsten van de ENSIA-zelfevaluatie opgenomen. Er wordt getoetst op opzet en bestaan (niet op werking). Voor DigiD worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder Logius/BZK.

DigiD:
DigiD is een authenticatiemiddel dat wordt ingezet voor onze digitale dienstverlening.

Niet voldaan voldaan

Website deurne.nl	Aanvragen van diensten van de gemeente	Geen risico's	
iBurgerzaken	Aanvragen van diensten van Burgerzaken (BRP en reisdocumenten)	Geen risico's	

Voor DigiD aansluitingen voldoet Deurne op alle punten aan de norm. Daarom zijn geen verbetermaatregelen gepland.

Getoetste collegeverklaring ENSIA - Suwinet

voldaan

Van onze ENSIA-zelfevaluatie worden jaarlijks twee onderdelen geaudit door een IT-auditor: DigiD en Suwinet. De basis voor de audit vormt de collegeverklaring. Hierin zijn de uitkomsten van de ENSIA-zelfevaluatie opgenomen. Er wordt getoetst op opzet en bestaan (niet op werking). Voor Suwinet worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder BKWI/SZW.

SUWI (Wet Structuur Uitvoeringsorganisatie Werk en Inkomen):
Suwinet is een digitale infrastructuur die is ontwikkeld door de Suwipartijen (UWV, SVB en gemeenten) om ervoor te zorgen dat zij gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak. Er worden alleen gegevens uitgewisseld waar een wettelijke grondslag voor is. Wij gebruiken Suwinet voor de uitvoering van de Participatiewet, de uitvoering van de IOAZ en IOAW, raadplegen van adresgegevens bij Burgerzaken en het raadplegen van gegevens door gemeentelijk gerechtsdeurwaarders wanneer er een getekend dwangbevel is.

Niet voldaan voldaan

Participatiewet/IOAZ/IOAW - Suwinet Inkijk	Gebruik Suwinet door Senzer	Geen risico's	

Voor het gebruik van Suwinet voldoet Deurne op alle punten aan de norm. Daarom zijn geen verbetermaatregelen gepland.

Status Basisregistratie Personen en Reisdocumenten

goed

Van onze zelfevaluatie ENSIA wordt de verantwoording over de Basisregistratie Personen (BRP) en de wet- en regelgeving voor de Reisdocumenten (paspoorten en ID-kaarten) afgeleid. De uitkomsten worden verzonden aan de Rijksdienst voor de Identiteitsgegevens (RvIG). De zelfevaluatie voor informatiebeveiliging vindt via de ENSIA systematiek plaats. De verantwoording over de kwaliteit van de registraties komt voort uit de zelfevaluatie in de Kwaliteitsmonitor.

De zelfevaluaties over informatiebeveiliging en de kwaliteit leiden tot scores. Gemeenten worden geacht de volgende score te behalen:

- BRP 1200 punten = 100%
- Reisdocumenten 1200 punten = 100%

0% - 75% 75% - 90% 90% - 100%

Basisregistratie Personen (BRP)
De zelfevaluatie BRP over het jaar 2021 is afgerond met 1120 punten van maximaal 1200.

93%

Wet- en regelgeving voor Reisdocumenten
De zelfevaluatie Reisdocumenten over het jaar 2021 is afgerond met 1140 punten van maximaal 1200.

95%

De belangrijkste verbetermaatregel die de gemeente zich voorneemt is het verstevigen van de controle op naleven van privacy-regelgeving (de AVG).

Status GEO-basisregistraties

goed

Wij verantwoorden ons aan het ministerie van BZK/Directoraat Generaal Bestuur, Ruimte en Wonen (DGBRW) over drie basisregistraties in het geografische domein. De rapportages zijn tot stand gekomen op basis van door ons uitgevoerde zelfevaluaties. De zelfevaluaties betreffen de kwaliteit van de registraties (geen informatiebeveiliging).

De zelfevaluaties over informatiebeveiliging en de kwaliteit leiden tot scores. Gemeenten worden geacht de volgende score te behalen:

- Basisregistratie Adressen en Gebouwen (BAG): norm is 75%
- Basisregistratie Grootschalige Topografie (BGT): norm, is 75%
- Basisregistratie Ondergrond (BRO): norm is 60%

0% - 74% 75% - 100%

Basisregistratie Adressen en Gebouwen (BAG)
De zelfevaluatie BAG over het jaar 2021 is afgerond met een score van 127 van maximaal 140 punten.

91%

Basisregistratie Grootschalige Topografie (BGT)
De zelfevaluatie BGT over het jaar 2021 is afgerond met een score van 100 van maximaal 110 punten.

91%

0% - 59% 60% - 100%

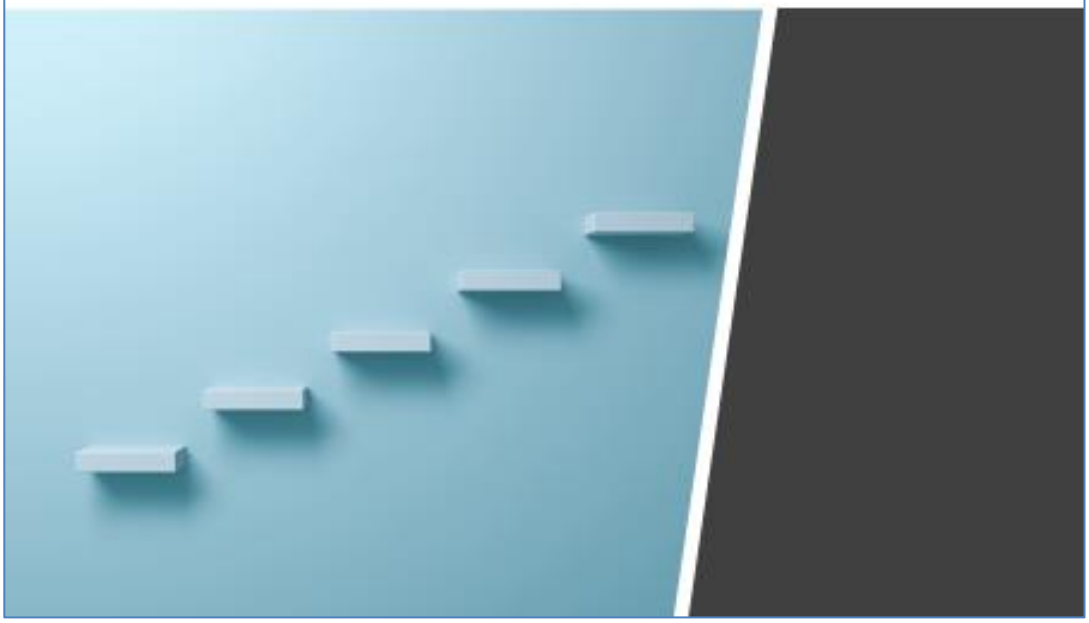
Basisregistratie Ondergrond (BRO)
De zelfevaluatie BGT over het jaar 2021 is afgerond met een score van 80 van maximaal 90 punten.

89%

Deurne voldoet aan de gestelde norm. Om dit vast te houden en verder te stroomlijnen zijn diverse procesverbeteringen gepland.

FG Jaarrapport 2021

Gemeente Deurne



Opgesteld door de Functionaris Gegevensbescherming (FG), januari 2022

Inleiding

In dit rapport laat de Functionaris Gegevensbescherming (FG) zien wat zijn bevindingen zijn over 2021 en geeft hij aanbevelingen.

Bijlagen

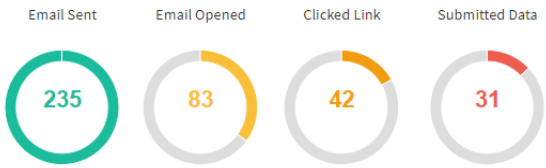
1. Overzicht datalekken 2021
2. Overzicht DPIA's

Deel 1. Terugblik op 2021

Het beeld van de FG is dat er in 2021 succesvol is gewerkt aan het verbeteren van gegevensbescherming binnen de gemeente Deurne.

Enkele voorbeelden van successen in 2021:

- In 2021 is de gemeente gestart met een tweejarig bewustwordingsprogramma. Stevig sturen heeft ervoor gezorgd dat veel medewerkers de e-learningmodules hebben gevolgd. Ook zijn medewerkers alerter gemaakt op het herkennen en melden van phishingmails. Aandacht hiervoor blijft nodig naast technische maatregelen om zoveel mogelijk te voorkomen dat medewerkers hierin trappen. De resultaten van de laatste phishingmailtest zijn:



- In Outlook is een knop "Rapporteren als phishing" opgenomen. Het melden van phishingmails bij de helpdesk is daardoor nog makkelijker geworden.
- De Privacy Officer/CISO en de FG werden in 2021 vaak en op tijd betrokken bij plannen voor nieuwe of gewijzigde processen met persoonsgegevens. De FG merkt dat er dan intern goed werd samengewerkt om gegevensbescherming meteen mee te nemen bij de inrichting van die nieuwe of gewijzigde processen. Het uitvoeren van (pre-)DPIA's aan de hand van het vastgestelde protocol uit 2020 wordt als nuttig ervaren.
- Medewerkers die een datalek hadden gemeld in 2021 kregen op het eind van het jaar een klein bedankje per post. Deze waardering werkt motiverend en stimuleert een open, veilige meldcultuur.
- De FG merkt dat er in 2021 goede regionale samenwerking was op het gebied van gegevensbescherming. Dat wierp zijn vruchten af. Zo resulteerde dat bijvoorbeeld in gezamenlijke privacy-afspraken met enkele gemeenschappelijke regelingen.

Bevindingen en aanbevelingen van de Functionaris Gegevensbescherming

BELEID

Het privacybeleid laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij heeft getroffen. De gemeente heeft een algemeen privacybeleid. Dat is vastgesteld in mei 2018. De afgelopen jaren is op diverse gebieden het algemeen privacybeleid uitgewerkt in protocollen, procedures etcetera.

⚠ Vaak is het onduidelijk wie eigenaar is van een proces en dus keuzes mag maken over gegevensbescherming binnen het proces. Het is daarom nodig om verantwoordelijkheden concreet te benoemen, te beleggen en vast te leggen.

Aanbeveling:

1.	Benoem proceseigenaren, leg dat vast en maak deze bekend binnen de organisatie. Beschrijf en leg aan hen uit wat deze verantwoordelijkheid inhoudt. Zodat zij hun rol met betrekking tot bescherming van persoonsgegevens actief kunnen oppakken.

PROCESSEN

Alle processen met persoonsgegevens horen privacyproof te zijn. Zo mogen bijvoorbeeld niet teveel gegevens verzameld worden of te lang bewaard. Daarnaast is het uitvoeren van een DPIA[1] vereist als een proces waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de persoonsgegevens zijn.

⚠ Of een bestaand proces met persoonsgegevens privacyproof is ingericht, is niet altijd duidelijk. In het verleden zijn namelijk niet alle processen voor inwerkingtreding aantoonbaar getoetst en privacyproof ingericht. De afgelopen 2 jaren is dit zichtbaar verbeterd voor nieuwe processen en gewijzigde processen met persoonsgegevens. Zo zijn er in 2020 en 2021 diverse DPIA's uitgevoerd en gesignaleerde risico's verkleind.

Aanbeveling:

2.	Er is een inhaalslag nodig om bestaande (ongetoetste) processen met persoonsgegevens aantoonbaar te toetsen en waar nodig privacyproof te maken. Aan te bevelen is om in 2022 daarmee aan de slag te gaan. Te beginnen met de processen met een hoog privacyrisico.

[1] **DPIA (Data Protection Impact Assessment)**
Een DPIA (Data Protection Impact Assessment) is een hulpmiddel om privacyrisico's van betrokkenen vooraf in kaart te brengen om vervolgens maatregelen te nemen zodat deze risico's worden beperkt.

ORGANISATIE

Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren. Het is van belang dat iedereen binnen de organisatie weet wat van hem of haar verwacht wordt op privacygebied.

⚠ De afgelopen jaren is op diverse gebieden het algemeen privacybeleid uitgewerkt in protocollen, procedures etcetera. Onduidelijk is of iedereen binnen de organisatie deze werkafspraken kent en toepast.

Aanbeveling:

3.	Toets of de werkafspraken bekend zijn binnen de organisatie. Verzorg trainingen als blijkt dat bijsturing nodig is.

⚠ In 2021 is het managementsysteem Cybermanager geïntroduceerd. Via het systeem kunnen managers beter monitoren en bijsturen op het gebied van privacy en informatieveiligheid. In 2021 zijn de informatiebeveiligingsnormen (ENSIA) toegevoegd in het systeem. Verdere implementatie is nodig zoals de aanvulling met privacynormen.

Aanbeveling:

4.	Ga verder met de implementatie van Cybermanager.

BETROKKENE

De gemeente hoort degene van wie zij persoonsgegevens verwerkt (de betrokkene) vooraf voldoende te informeren over wat zij gaat doen met diens gegevens. De gemeente zorgt daarnaast dat een betrokkene in staat wordt gesteld om controle te houden over zijn of haar gegevens. Bijvoorbeeld door op verzoek inzage te bieden.

⚠ Om betrokkenen beter te informeren is het aan te raden om de privacyverklaring op de gemeentelijke website te herzien. Een interne privacyverklaring voor medewerkers van de gemeente ontbreekt.

Aanbeveling:

5.	Herzie de privacyverklaring op de gemeentelijke website. Stel een interne privacyverklaring op.

SAMENWERKING

De gemeente werkt veel samen met derde partijen. Daarbij worden persoonsgegevens gedeeld. 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.

⚠ Er is achterstallig werk in de administratie en beheer van contracten met derde partijen over gegevensbescherming. Onduidelijk is of afspraken met derde partijen ontbreken, of gemaakte afspraken nog actueel zijn en of ze worden nageleefd. Afspraken die in een la verdwijnen voegen niets toe aan de veiligheid van gegevens. Het is daarom nodig om de papieren werkelijkheid ook daadwerkelijk om te zetten in tastbare gegevensbescherming. De gemeente blijft eindverantwoordelijk bij het uitbesteden van publiekrechtelijke taken aan derde partijen.

Aanbeveling:

6.	Zorg voor een actueel totaaloverzicht van afspraken met derde partijen. Maak afspraken met derde partijen als deze ontbreken. Actualiseer bestaande afspraken met derde partijen indien nodig. Ga na of de gemaakte afspraken worden nageleefd en vraag de derde partij om daar periodiek verantwoording over af te leggen.

BEVEILIGING

Passende technische en organisatorische maatregelen zijn nodig om persoonsgegevens te beveiligen. Het is verplicht meldenswaardige datalekken te melden aan de Autoriteit Persoonsgegevens en betrokkenen.

⚠ Op 28 oktober 2021 stuurde VNG voorzitter Jan van Zanen een oproep aan alle burgemeesters in Nederland om met het College, Raad en ambtelijke organisatie de benodigde tijd, mensen en middelen vrij te maken om de digitale beveiliging van gemeenten in lijn te brengen met de actuele risico's van ransomware. Hij riep op de onderstaande maatregelen te gaan treffen:

	Maatregel	De CISO van de gemeente Deurne geeft in november 2021 aan:
	Houd hard- en software up-to-date	*Dat heeft de aandacht heeft van systeem- en functioneel beheerders. Veel extern bereikbare software binnen de gemeente is uitbesteed. Leveranciers houden deze software goed bij.*
	Gebruik meerfactorauthenticatie	*Gebruik van meerfactorauthenticatie is ingevoerd voor alle toegang buiten het eigen netwerk*

	Hanteer een strikte netwerksegmentatie	*Het netwerk is logisch in "kamers" verdeeld maar alle "deuren" daartussen staan open. Een aanvaller kan eenmaal binnen overal rondlopen.*
	Zorg voor robuuste back-ups	*Back-up voorzieningen zijn waarschijnlijk in orde maar overzicht, controle en beleid hierover ontbreken.*
	Test en oefen uw ICT-crisisplan(nen)	*Deurne beschikt nog niet over ICT-crisisplan(nen).*

Aanbeveling:

7.	Zorg voor strikte netwerksegmentatie. Zorg voor overzicht, controle en beleid over back-ups. Maak, test en oefen met ICT-crisisplannen.

⚠ Een loggingsbeleid en uitvoering daarvan ontbreekt.

Aanbeveling:

8.	Zorg voor een loggingsbeleid en uitvoering daarvan. Loggegevens periodiek controleren is aan te raden om beveiligingsincidenten (waaronder datalekken) tijdig te ontdekken. Tijdige ontdekking kan de impact van een incident verkleinen. Daarnaast kan ervan geleerd worden zodat toekomstige incidenten worden voorkomen.

VERANTWOORDING

Het is de verantwoordelijkheid van de gemeente om aantoonbaar te maken dat zij voldoet aan de AVG-verplichtingen (verantwoordingsplicht).

⚠ Op dit moment kan de gemeente onvoldoende aantoonbaar maken dat zij voldoet aan alle AVG-verplichtingen. Eén van de oorzaken is dat in het verleden niet alle bestaande processen voor inwerkingtreding aantoonbaar getoetst en privacyproof ingericht zijn. Daarnaast wordt het verwerkingsregister onvoldoende onderhouden. De gemeente heeft dus nog onvoldoende zicht en grip op al haar verwerkingen van persoonsgegevens.

Aanbeveling:

9.	Aan te bevelen is om in 2022 aan de slag te gaan met het actualiseren van het verwerkingsregister. Te beginnen met de processen met een hoog privacyrisico.

Wet politiegegevens (Wpg)

In 2021 bleek dat de gemeente Deurne naast de AVG-verplichtingen ook rekening moet houden met de verplichtingen uit de Wet politiegegevens (Wpg). Dat komt omdat zij werkgever is van opsporingsambtenaren, namelijk leerplichtambtenaren en deze verwerken politiegegevens. Eén van de eisen uit de Wpg is een jaarlijkse interne audit en om de vier jaar een externe audit. Deze externe audit is voor het eerst uitgevoerd in 2021. Het externe auditrapport gaat naar de Autoriteit Persoonsgegevens.

⚠ De externe audit liet zien dat er nog verbeteringen nodig zijn om te gaan voldoen aan de Wpg.

Aanbeveling:

10.	Maak een verbeterplan naar aanleiding van het externe auditrapport en voer de benodigde verbeteringen door in 2022. Zorg dat de interne Wpg-audit uitgevoerd wordt in 2022.

Deel 2. Vooruitkijken naar 2022

In deel 1 werd duidelijk dat in 2021 (en 2020) succesvol is gewerkt aan het verbeteren van gegevensbescherming bij nieuwe en gewijzigde processen. Goed om dat vast te houden en in 2022 aan de slag te gaan om meer zicht en grip te krijgen op bestaande verwerkingen van persoonsgegevens en politiegegevens. Achterstallig werk oppakken dus.

De FG heeft 10 aanbevelingen gedaan in deel 1. Gezien de huidige beperkte capaciteit aan mensen en middelen is het realistisch dat niet alles in 2022 opgepakt kan worden. Aan te raden is om de capaciteit uit te breiden zodat sneller zaken op orde kunnen komen en risico's beter worden beheerst. Voor 2022 ziet de FG de volgende 3 prioriteiten:

1. Verwerkingsregister actualiseren

- Ga aan de slag om het verwerkingsregister te actualiseren en borg het beheer ervan. Op dit moment wordt het register onvoldoende onderhouden waardoor het register onbetrouwbaar is. Zorg dat nieuwe en gewijzigde verwerkingen na aantoonbare toetsing opgenomen worden in het register. Zorg voor een overzicht van verwerkingen met een hoog privacyrisico in het verwerkingsregister.

2. Impact cyberaanval verkleinen

- Zorg voor strikte netwerksegmentatie. Zorg voor overzicht, controle en beleid over back-ups. Maak, test en oefen met ICT-crisisplannen om zo goed mogelijk voorbereid te zijn op een mogelijke cyberaanval. Zorg voor een loggingsbeleid en uitvoering daarvan om incidenten tijdig te ontdekken.

3. Wet politiegegevens (Wpg) naleven

- Maak een verbeterplan naar aanleiding van het externe auditrapport en voer de benodigde verbeteringen door in 2022. Zorg dat de interne Wpg-audit uitgevoerd wordt in 2022.

Bijlage 1 - Overzicht datalekken 2021

Hieronder staan alle aan de gemeente gemelde incidenten in verband met persoonsgegevens uit 2021. Deze zijn gemeld door medewerkers of externe partijen.

De gemeente heeft corrigerende en preventieve maatregelen getroffen. Meldingen aan de Autoriteit Persoonsgegevens (AP) en/of betrokkenen werden uitgevoerd na beoordeling dat er een mogelijk privacyrisico aanwezig was voor de betrokkenen.

Nr	Omschrijving incident
1	Bouwtekeningen zijn onvoldoende geanonimiseerd gemaild naar een betrokken architect.
2	Laptop gestolen uit een auto.
3	Netwerkinbraak GR Senzer (ransomware-aanval).
4	Door de gemeente onjuist geanonimiseerde gepubliceerde stukken over een omgevingsvergunning zijn door OpenArchivaris.nl geïndexeerd en als kopie te downloaden.
5	Brief met gegevens van een verkeerde cliënt is verstuurd naar een incassobureau.
6	Bij het versturen van opgevraagde vergunningen aan een inwoner zijn persoonsgegevens niet volledig weggelakt.
7	Een onnodige kopie ID-bewijs werd ingeleverd door een inwoner bij een omgevingsvergunning via het omgevingsloket en is doorgezet naar GR VRBZO.
8	Een afbeelding van een gevonden identiteitskaart en rijbewijs is gepubliceerd op de website VerlorenofGevonden.nl.
9	Een brief met naam en geboortedatum van de verkeerde jongere is naar ouders gestuurd.
10	Een groepsmail over een uitnodiging voor een netwerkbijeenkomst is per ongeluk niet verstuurd via BCC.
11	Een planschadeovereenkomst is per ongeluk aan de verkeerde inwoner toegestuurd.
12	Brieven met bevestiging van geboorteaangifte waren niet bezorgd bij de ouders.
13	Een medewerker van Zorg in Deurne ging op huisbezoek. Omdat er niemand thuis was, laat deze een briefje achter in de brievenbus en schrijft daarop de naam van de cliënt en dat Zorg in Deurne langs is geweest. Vervolgens komt de medewerker er achter dat deze in de verkeerde straat staat.

Aard van de incidenten

De meeste aan de gemeente gemelde incidenten in 2021 gingen over persoonsgegevens die onbedoeld terecht zijn gekomen bij onbevoegden.

Verloopoverzicht meldingen

	2018	**2019**	**2020**	**2021**
Gemeld aan/binnen de gemeente	8	10	15	13
Gemeld aan de AP	3	5	4	4

Bijlage 2 - Overzicht DPIA's 2021

Onderwerp DPIA	Status eind 2021
Zaaksysteem Onegov	DPIA uit 2019. Maatregelen om privacyrisico's te beperken moeten nog afgerond worden.
Zorg- en veiligheidshuis (ZVH)	DPIA uit 2019. Maatregelen om privacyrisico's te beperken moeten nog afgerond worden.
Cameratoezicht gemeentehuis	DPIA uit 2021. Afgerond in 2021.
Jongeren in kwetsbare posities (JIKP)	DPIA uit 2021. Afgerond in 2021.
Agressieprotocol	DPIA uit 2021. Maatregelen om privacyrisico's te beperken moeten nog afgerond worden.
Wijziging Wgs/vroegsignalering/Grip op Schuld	DPIA is in behandeling.
Wet inburgering	DPIA is in behandeling.
Jeugd en Gezinswerk	DPIA wordt nog gestart.
GPS tracker op voertuigen buitendienst	DPIA wordt nog gestart.
Powerbrowser	DPIA wordt nog gestart.
Financieel systeem	DPIA wordt nog gestart.
E-formulieren leerlingenvervoer en gehandicaptenparkeerplaats op de website	FG heeft op 16-12-2020 een DPIA geadviseerd.