Jaarrapportage FG 2022
Gegevensbescherming AVG

Voor:

Het college van Burgemeester en Wethouders van de gemeente Druten

Het college van Burgemeester en Wethouders van de gemeente Wijchen

Het bestuur en de directie van de Werkorganisatie Druten Wijchen

Van:

Lotte Livius	Functionaris gegevensbescherming AVG
Maaike van Walstijn	wnd. Functionaris gegevensbescherming AVG

Datum: 1 maart 2023

Vastgesteld door:

Inhoud

Inleiding en samenvatting 3
Leeswijzer 4
A. Uitslagen VNG-borgingsinstrument 5
1. Privacybeleid 5
2. Processen 5
3. Organisatorische inbedding....7
4. Rechten van betrokkenen 8
5. Samenwerking....9
6. Beveiliging....10
7. Verantwoording....10
B. Kencijfers Privacy 2021-2022....12
1. Toelichting DPIA's....12
2. Toelichting Datalekken en beveiligingsincidenten 12
3. Toelichting Rechten van betrokkenen 13
4. Toelichting Klachten van betrokkenen 13
5. Aantal Fte's 14
C. Advies 2023....15
Bijlage Definities 17

Inleiding en samenvatting

Gemeenten verwerken op grote schaal informatie en persoonsgegevens, niet alleen van inwoners maar ook van medewerkers en relaties van de gemeente. Zonder deze gegevens kunnen wij onze taken niet uitvoeren. Onder verantwoordelijkheid van de colleges van Burgemeester en Wethouders, de gemeenteraden en het bestuur van de WDW (de 'verwerkings-verantwoordelijken') vinden vele verwerkingen van persoonsgegevens plaats. Zij zijn belast met de uitvoering van regelgeving en hiervoor bestuurlijk verantwoordelijk.

In de Europese Algemene Verordening Gegevensbescherming (AVG) wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dienen we transparant te zijn welke persoonsgegevens we verwerken, voor welk doel en op welke grondslag. Tijdens hun levensduur moeten persoonsgegevens adequaat worden beveiligd, mogen ze niet zomaar voor een ander doel worden verwerkt en moeten na afloop worden vernietigd of geanonimiseerd. De Baseline Informatiebeveiliging Overheid (BIO) waarborgt de betrouwbaarheid van informatie (en gegevens) en geeft organisatorische en technische maatregelen aan die genomen moeten worden om de risico's bij het verwerken te beperken. Daarnaast hebben we ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in onze organisatie.

Hier wordt extern en intern toezicht op gehouden. De Autoriteit Persoonsgegevens (AP) houdt extern toezicht op de naleving van de privacywetgeving. De Functionaris Gegevensbescherming AVG (FG) en de Chief Information Security Officer (CISO) zien er intern op toe dat voldaan wordt aan de verplichtingen uit de AVG en de BIO. De FG en CISO rapporteren hun bevindingen rechtstreeks aan de colleges van burgemeester en wethouders en het bestuur van de Werkorganisatie Druten Wijchen (WDW).

In dit jaarverslag kunt u lezen wat de FG in 2022 heeft waargenomen als het gaat om de bescherming van persoonsgegevens onder de AVG. Het is opgesteld aan de hand van het AVG-borgingsinstrument, ontwikkeld door de VNG Realisatie en de Informatiebeveiligingsdienst (IBD).[1] Het instrument is bedoeld om de AVG-normen te vertalen naar een kwaliteitscyclus voor gegevensbescherming in de gemeentelijke processen. Hiermee krijgen gemeenten concrete handvatten om de goede omgang met persoonsgegevens in de gehele organisatie te waarborgen. Het maakt inzichtelijk wat op orde is en wat nog niet.

Het instrument is eind 2022 ingevuld. Hieruit blijkt dat de organisatie op sommige punten goed scoort maar dat nog vele beheersmaatregelen genomen moeten worden. Het wettelijk vereiste volwassenheidsniveau 3 wordt zeker nog niet gehaald.

[1] Zie het document 'Criteria borging AVG / Borgingsproduct gegevensbescherming in de gemeentelijke organisatie'.

Deze conclusies sluiten aan bij de conclusies in het regionale rekenkamer-onderzoek naar de informatiebeveiliging en privacybescherming (AVG) in Wijchen, en komen ook overeen met de bevindingen van de externe audit naar de Wet politiegegevens (Wpg).[2]

Samenvattend hebben we in 2022 een goed begin gemaakt om gegevensbescherming de aandacht te geven die het verdient. Vanuit alle hoeken van de organisatie komen privacyvraagstukken steeds vaker op de juiste plek terecht. Adequaat omgaan met persoonsgegevens is een blijvend proces en vergt aandacht van medewerkers, management en bestuur. De uitdaging is om die aandacht vast te houden en te benutten en actief aan de slag gaan met gegevensbescherming en compliancy.

Leeswijzer

Deze jaarrapportage bestaat uit drie onderdelen. In deel A wordt de stand van zaken toegelicht aan de hand van de thema's uit het borgingsproduct:

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording

In deel B van de rapportage worden de belangrijkste kencijfers voor gegevensbescherming in 2022 toegelicht. Het rapport sluit af met een advies welke stappen u in 2023 zou kunnen nemen om gegevensbescherming daadwerkelijk te verbeteren en te borgen in de organisatie.

Notabene

1. Waar in dit rapport wordt gesproken over 'de organisatie' worden zowel de gemeente Druten, de gemeente Wijchen als de Werkorganisatie Druten Wijchen bedoeld.

2. Het borgingsinstrument en dit rapport zijn in november 2022 voorbereid door de Functionaris Gegevensbescherming Lotte Livius, en aangevuld door de waarnemend Functionaris Gegevensbescherming.

20 november 2022,

Lotte Livius
Functionaris Gegevensbescherming

7 maart 2023,

Maaike van Walstijn
wnd. Functionaris
Gegevensbescherming

[2] De Wpg is een Nederlandse wet die specifiek gericht is op de verwerking van politiegegevens. De wet stelt regels aan hoe opsporingsinstanties zoals boa's persoonsgegevens mogen verwerken, bewaren en delen met andere instanties. Hoewel de AVG en de Wpg verschillende wetgevingen zijn met eigen specifieke doelen en vereisten, delen ze wel hetzelfde uitgangspunt: de bescherming van persoonsgegevens. Beide wetten hebben als doel om ervoor te zorgen dat organisaties de privacy van betrokkenen respecteren en waarborgen dat persoonsgegevens op een veilige en verantwoorde manier worden verwerkt.

A. Uitslagen VNG-borgingsinstrument

1. Privacybeleid

Het privacybeleid is het kader waarin een organisatie aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe zij omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving. Periodiek wordt gecontroleerd of de verwerkingen in lijn zijn met het privacybeleid en de geldende wet- en regelgeving.

Er is een getoetst en vastgesteld privacybeleid dat geldt voor de gemeenten Druten en Wijchen, en de WDW. Bezoekers van de websites worden via drie (identieke) privacy-verklaringen geïnformeerd over hoe de organisaties globaal omgaan met hun persoonsgegevens, hoe zij hun rechten onder de AVG kunnen uitoefenen, en het gebruik van cookies.

In de loop van de tijd zijn additionele afspraken gemaakt hoe om te gaan met persoonsgegevens van 'internen' zoals medewerkers, gemeenteraadsleden en extern ingehuurden. Deze afspraken moeten worden vastgesteld en opgenomen in een nieuwe versie van het privacybeleid. Het verdient aanbeveling om ook domein-specifieke regels op te nemen in het beleid, dat wil zeggen de regels hoe het desbetreffende domein omgaat met (sectorspecifieke) wet- en regelgeving, persoonsgegevens en gegevensbescherming. Sommige teams in de organisatie beschikken overigens al wél over een specifieke privacyregeling.

Geconstateerd moet worden dat er inderdaad privacybeleid is maar dat dit nog niet leidend is bij het starten van nieuwe verwerkingen, de aankoop of ontwikkeling van nieuwe informatievoorzieningen. Deze worden lang niet altijd voorafgaand getoetst aan het privacybeleid of de AVG.

2. Processen

Volgens de AVG moeten alle werkprocessen waar persoonsgegevens in worden verwerkt (vrijwel allemaal dus) worden ingericht aan de hand van de AVG-voorschriften. Iedere verwerking moet berusten op wettelijke grondslag, een helder doel hebben, alleen werken met de noodzakelijke en juiste gegevens (kwaliteit en dataminimalisatie) en na de verwerkingstermijn worden vernietigd of geanonimiseerd.

Op hoofdlijnen zijn onze **werkprocessen** in beeld en beschreven maar slechts een enkele maal is daarin expliciet aandacht voor gegevensbescherming. Binnen de domeinen is veelal wel bekend wat de hoog-risico-verwerkingen zijn maar de implicaties daarvan voor het werk en de medewerkers niet. Protocollen en

werkinstructies ontbreken meestal. Het ontbreekt ook aan een uniform proces om persoonsgegevens periodiek te verwijderen of te anonimiseren.

De organisatie voldoet deels aan de verplichting om een **register** bij te houden van alle verwerkingsactiviteiten (art. 30 AVG). Er worden momenteel vier registers bijgehouden: één voor de verwerkingsverantwoordelijken in Druten, één voor Wijchen en één voor de WDW.
Al die verwerkingen zijn tevens opgenomen in een overall register. De registers zijn opgezet volgens de wettelijke eisen die daarvoor gelden, dat wil zeggen dat de doeleinden, categorieën persoonsgegevens, betrokkenen, ontvangers, bewaartermijnen, doorgifte en technische en organisatorische maatregelen opgenomen kunnen worden. Desgevraagd kunnen (d.w.z. moeten) de registers ter beschikking worden gesteld aan de Autoriteit Persoonsgegevens.

Uit de registers blijkt echter ook dat niet alle verwerkingen afdoende beschreven zijn, en dat de risico's van de verwerkingen niet goed in beeld zijn. Onduidelijk is of alle verwerkingen wel opgenomen zijn, of juist onterecht verwerkingen staan opgenomen die niet meer uitgevoerd worden. De oorzaak hiervan is dat het **beheer** van de registers niet is ingeregeld: er zijn geen proceseigenaren die hun verwerkingen wijzigen, nieuwe verwerkingen toevoegen of oude verwijderen. Voor zover mogelijk neemt de FG nu deze verantwoordelijkheid op zich maar het dringende verzoek is deze te beleggen bij de proceseigenaren in de organisatie, alleen zij hebben immers het overzicht.

Een ander belangrijk vereiste is het uitvoeren van Data Protection Impact Assessments (**DPIA**). Hiervoor scoren we redelijk maar nog niet voldoende. Een DPIA is een instrument om vóórdat de gegevensverwerking start (de dienstverlening start of een applicatie in gebruik wordt genomen) de privacy-risico's in kaart te brengen, de maatregelen te benoemen om die risico's te verkleinen en de afwegingen daarover vast te leggen (transparant & accountable). Een DPIA is verplicht voor alle verwerkingen die vermoedelijk een hoog risico voor betrokkenen met zich mee brengen, en voor de onderwerpen die zijn aangewezen door de AP (zoals cameratoezicht).

Er is een redelijk overzicht van de DPIA's die tot heden zijn uitgevoerd en in 2022 zijn al aanzienlijk meer DPIA's uitgevoerd dan in 2021. Geconstateerd moet echter worden dat die rapportages niet allemaal geregistreerd zijn en niet makkelijk terug te vinden. Ook zijn er nog vele verwerkingen waar een DPIA ontbreekt of waarvan het DPIA-proces pas start als de verwerking al wordt. Dat moet echt anders.

Het advies is om proceseigenaren het verwerkingenregister te laten controleren en een overzicht te laten maken van de meest risicovolle verwerkingen. De resulterende lijst kan geprioriteerd worden, en (zo nodig) gestart worden met het uitvoeren van DPIA's. Op deze wijze zorgen we dat de grootste risico's beperkt kunnen worden, maar ook dat het werkbaar blijft en gegevensbescherming al doende wordt geborgd in de organisatie.

3. Organisatorische inbedding

Het is van belang dat eenieder het belang van privacy ziet en onderschrijft, op de hoogte is van de wet- en regelgeving en deze ook daadwerkelijk in praktijk brengt (kan brengen) bij het werk. Organisatorische inbedding betekent naast bewustwording (awareness) ook het toewijzen van **rollen**, **taken, verantwoordelijkheden en bevoegdheden** met betrekking tot privacy.

Op dit gedeelte wordt wisselend gescoord. De organisatie scoort goed wat betreft de **FG**: deze is aangesteld en aangemeld bij de Autoriteit Persoonsgegevens (voor de AVG). De FG weet wat behoort tot haar takenpakket (informeren, adviseren en toezicht houden) en heeft voldoende middelen om de deskundigheid op peil te houden. Om de rol als interne toezichthouder echt goed te kunnen vervullen, is het cruciaal dat de FG wordt betrokken bij alle aangelegenheden die verband houden met gegevensbescherming (bijvoorbeeld ook bij het voornemen een nieuwe IT-systeem aan te schaffen). Dat laat nog te wensen zover.

Als het gaat om de verantwoordelijkheden op het niveau van de **lijnmanagement** (domeinmanagers) wordt er wisselend gescoord. De domeinmanager is feitelijk verantwoordelijk voor de omgang met persoonsgegevens in zijn/haar domein (proceseigenaar). In de praktijk is dit niet altijd merkbaar. Het is aan te bevelen om privacy-gerelateerde taken en verantwoordelijkheden uit te werken, deze vast te leggen (privacy governance met RACI-schema) en daadwerkelijk op die wijze uit te voeren. Dit vergt uiteraard tijd om te implementeren en zal goed gecommuniceerd moeten worden. Trainingen kunnen helpen bij de implementatie hiervan, daar kan ik als FG zeker aan bijdragen.

Over het algemeen is er binnen de organisatie redelijk **algemene kennis** over privacy en de AVG. Medewerkers zijn redelijk goed op de hoogte hoe ze adequaat met persoonsgegevens om moeten gaan. Door middel van e-learning worden trainingen gegeven over het belang van privacy & informatieveiligheid. Uiteraard is er altijd ruimte voor verbetering, maar op dit terrein scoort de organisatie een voldoende. De vraag is wel of er voldoende **middelen** beschikbaar zijn om privacybescherming te bevorderen in kennis, houding en gedrag van medewerkers. Zo is op afdelingsniveau lang niet altijd een protocol, procedure of werkinstructie beschikbaar over de adequate omgang met persoonsgegevens specifiek voor dat terrein. Op dit punt scoren we dan ook gedeeltelijk voldoende/onvoldoende.

De organisatie scoort redelijk goed omdat op (vrijwel) alle afdelingen **privacy-ambassadeurs** zijn. Zij fungeren als eerste aanspreekpunt voor hun directe collega's, verzamelen privacy-gerelateerde vragen en zijn op de hoogte van de ontwikkelingen binnen de eigen afdeling. Theoretisch kunnen privacy-vragen zo snel en doelmatig opgepakt worden, en worden de zwaardere vraagstukken naar

het niveau van het lijnmanagement, de FG (of PO) getild. In praktijk werkt het echter niet zo. De privacy-ambassadeur is geen officiële rol, de ambassadeur heeft geen uren beschikbaar om deze werkzaamheden te vervullen, en nog geen privacy-training gehad om deze rol goed te vervullen. Ook zijn er slechts ad hoc gesprekken tussen de FG en individuele privacy-ambassadeurs. Het advies is om deze rol te formaliseren, ervoor te zorgen dat er voor iedere afdeling een dergelijk aanspreekpunt is, dat diegene ook beschikt over uren en mogelijkheden heeft zijn/haar privacy-kennis voldoende op peil te houden.

De organisatie scoort onvoldoende om ten minste één **privacy-adviseur** te hebben die beschikt over ruime kennis over privacywet- en regelgeving in de gemeentepraktijk (ook wel Privacy Officer of PO genoemd). Er wordt ad hoc soms wat capaciteit voor vrij gemaakt maar deze taak is nog niet structureel belegd. Vaak wordt daarom een beroep gedaan op de FG, die daarmee feitelijk een oneigenlijke taak vervult en waardoor de toezichtstaak in het gedrang komt. Van het gebruikelijke 'drie ogen-principe ('three lines of defence' of 3-LoD)[3] komt zo terecht. Het is van belang dat er ruimte wordt gemaakt voor een privacy-adviseur. Deze kan op casusniveau adviseren over adequate bescherming en verwerking van persoonsgegevens terwijl de FG toezicht houdt.

Medewerkers van de WDW hebben enkel toegang tot de systemen en gegevens die zij nodig hebben voor de uitvoering van hun werkzaamheden. Hiervoor zijn **autorisatieschema's** vastgesteld en de organisatie hanteert een procedure Autorisatie en controle toegangsrechten. Als een medewerker uit dienst treedt, worden diens autorisaties zo snel mogelijk verwijderd. Dat zou op dezelfde wijze moeten worden ingeregeld bij een verandering van functie. Wel worden alle autorisaties periodiek gecontroleerd.

4. Rechten van betrokkenen

Organisaties zijn verplicht om transparant en in eenvoudige taal uit te leggen aan de betrokkenen (d.w.z. degenen van wie de persoonsgegevens verwerkt worden) hoe hun persoonsgegevens verwerkt worden, en wel voordat de verwerking start. Ook moeten betrokkenen in staat zijn om hun rechten uit te oefenen. Zo hebben ze het recht om persoonsgegevens in een digitaal leesbaar standaardformaat te ontvangen (dataportabiliteit), het recht op correctie, verwijdering en beperking; verder kunnen betrokkenen bezwaar maken tegen de verwerking of een klacht indienen[4].

Bezoekers van de websites van de gemeenten Druten, Wijchen en de Werkorganisatie Druten Wijchen kunnen daar de **privacyverklaring** vinden met een korte beschrijving van hun rechten, de manier hoe zij een verzoek kunnen indienen en hoe de FG gecontacteerd kan worden. Wanneer er een verzoek

[3] Zie definities in bijlage voor een omschrijving van het model.
[4] Artikel 12 t/m 23 AVG.

wordt ingediend, wordt dit nu afgehandeld door een medewerker van Algemeen Juridische Zaken (AJZ), de FG en het team Informatiebeheer ondersteunen hierin. De wettelijke termijnen van de verzoeken worden bewaakt. Dit proces verloopt goed, Idealiter zou het afhandelingsproces ondersteund worden met automatisering. Een systeem dat de afhandeling van rechten van betrokkene goed ondersteund, is er echter nog niet, dat wordt nog ontwikkeld. Voorafgaand aan een eventuele ingebruikname van zo'n systeem zal overigens wel een DPIA moeten worden uitgevoerd.

Het advies is de privacy-verklaringen op de websites wel wat gemakkelijker vindbaar te maken op de website, een **procesbeschrijving Rechten betrokkenen op te stellen en** een organisatie-breed **communicatieplan** te maken over privacy waarin structureel rekening wordt gehouden met de wettelijke transparantieverplichtingen.

5. Samenwerking

De organisatie scoort redelijk goed als het gaat om samenwerking. We werken op veel gebieden samen met (mede)overheden, ketenpartners en private organisaties. Daarbij is al snel sprake van het verwerken van persoonsgegevens (verzamelen, ontvangen, verstrekken van gegevens). Ook hier moeten we uiteraard volledig voldoen aan de AVG. We moeten dan vooral schriftelijke afspraken maken met partijen en daarbij expliciet aandacht besteden aan gegevensbescherming.

We hebben redelijk goed inzichtelijk welke partijen persoonsgegevens van ons ontvangen en andersom. Er zijn verschillende convenanten en samenwerkingsovereenkomsten afgesloten met (keten)partners (art. 26 AVG **gezamenlijke verwerkingsverantwoordelijken**). Bij het inschakelen van externe partijen worden gelukkig ook steeds vaker **verwerkers-overeenkomsten** afgesloten (en door de FG vastgelegd in het register).

Toch is het ook hier nodig om verbeteringen door te voeren. Te vaak gaan medewerkers een contract aan en wordt pas achteraf de verwerkersovereenkomst nog opgesteld, soms ontbreekt de hoofdovereenkomst helemaal en zijn de afdelingen AJZ en Inkoop niet eens betrokken. Hierdoor zitten we soms vast aan ongewenste contractverplichtingen, is het contract soms aangegaan door de 'verkeerde' partijen (die ons echter wel binden), is de GIBIT niet van toepassing en voldoet de verwerker niet aan de minimale beveiligingseisen.

Het dringende advies is dit snel te verbeteren. Idealiter is er ook één verzamelpunt waar alle convenanten en verwerkersovereenkomsten bewaard en beheerd worden. Ook zou er eenvoudig een overzicht moeten kunnen worden gegenereerd van alle gegevensverwerkingen waar we medeverantwoordelijk voor zijn en van persoonsgegevens die we verstrekken.

Als het gaat om **eenmalige verstrekking** van persoonsgegevens wordt die vrijwel altijd getoetst aan relevante wetgeving en de beginselen van de AVG. Hierin scoren we goed. Een verbeterpunt is om bij ad hoc bevragingen vooraf duidelijkheid te krijgen over de rol van de ontvanger. Hiervoor zou een werkinstructie gemaakt moeten worden en zo nodig ook afspraken gemaakt worden met de ontvanger, bijvoorbeeld over de geheimhouding.

6. Beveiliging

Verwerkingsverantwoordelijken hebben de plicht om passende technische en organisatorische maatregelen te nemen om persoonsgegevens goed te beschermen. Dit vloeit voort uit het behoorlijkheidsbeginsel, integriteitsbeginsel en het vertrouwelijkheidsbeginsel. Daarnaast geldt ook onder de AVG een meldplicht voor 'datalekken'. Dit houdt in dat inbreuken op (de beveiliging van) persoonsgegevens geregistreerd moeten worden en soms ook gemeld aan de AP en/of de betrokkenen (artikelen 32 - 34 AVG.)

Op het gebied van **informatieveiligheid** scoren we in het algemeen goed. Er is een autorisatieprocedure voor het in- en uittreden van medewerkers, deze wordt ook periodiek getoetst. De organisatie treft **passende technische en organisatorische maatregelen** om persoonsgegevens adequaat te beschermen, en deze periodiek test en evalueert. Vervolgstap die hierin gemaakt moet worden is om expliciet aandacht te besteden aan privacy-specifieke beveiligingseisen, Privacy by Design en Privacy by Default (PbDD). Gemeentelijke medewerkers zijn vaak niet bekend met privacy-specifieke beveiligingseisen die relevant zijn voor hen.

Data-incidenten worden gelukkig steeds vaker gemeld. Het aantal (meldingen van) datalekken neemt dan ook toe. In dit stadium moeten we daar vooral blij mee zijn. Alleen dan kunnen we maatregelen treffen om de beveiliging te verbeteren en de gevolgen voor betrokkenen minimaliseren. Toch is er wel enige reden voor bezorgdheid. Medewerkers zijn niet altijd voldoende op de hoogte wat (potentieel) een datalek vormt en weten niet altijd precies bij wie ze dat moeten melden en wat er vervolgens moet gebeuren. Een procesbeschrijving hoe om te gaan met data-incidenten is aan te bevelen.

Voor een verdere toelichting over de stand van zaken van informatiebeveiliging verwijs ik hierbij naar het jaarplan van de CISO en de ENSIA-auditrapportages.

7. Verantwoording

Onder de AVG moeten verwerkingsverantwoordelijken zich niet alleen houden aan de regels, maar ook kunnen aantonen dat ze zich eraan houden (transparant en '**accountable'**). Hierop wordt wisselend gescoord. De WDW heeft een redelijk up-to-date verwerkingsregister, er zijn verschillende Data Protection Impact Assessments (DPIA's) uitgevoerd en steeds vaker komt de vraag uit de

organisatie of er wellicht een DPIA moet worden uitgevoerd. Dat is goed nieuws.

Organisatiebreed en op afdelingsniveau is nog onvoldoende inzicht in de high-risk-verwerkingen en de DPIA's die al zijn (en zouden moeten worden) uitgevoerd. DPIA's worden ook lang niet altijd formeel vastgesteld, dat zou wel moeten. Een risicomanagement-proces ontbreekt, maatregelen worden niet planmatig opgepakt. Op afdelingsniveau worden zelden GAP-analyses uitgevoerd naar de stand van zaken van gegevensbescherming. Het advies is dit in 2023 te gaan doen. Het is anders niet goed mogelijk om onze compliancy en verbetermaatregelen aan te tonen (en gegevensbescherming naar een hoger niveau te tillen).

Een van de zaken die in 2023 goed onderzocht zou moeten worden is de **toestemming** van betrokkene voor de verwerking van gegevens. We hebben niet inzichtelijk welke verwerkingen plaatsvinden op basis van toestemming. Toestemming is weliswaar een geldige grondslag om gegevens te mogen verwerken onder de AVG, maar deze grondslag is niet of nauwelijks bruikbaar voor een overheidsorganisatie of werkgever. Voor zover in onze organisatie gegevensverwerkingen toch rechtmatig plaatsvinden op basis van toestemming, moeten we t kunnen aantonen dat er sprake is van volwaardige, expliciete toestemming, dat de betrokkene voldoende geïnformeerd was en waarmee. Hiervoor moeten we een systematiek ontwikkelen.

Bij verantwoording hoort uiteraard ook **toezicht**. Toezicht moet structureel onderdeel zijn van de werkprocessen. Er zal gerapporteerd moeten worden of gegevensverwerkingen rechtmatig plaatsvinden. En hoewel u hier de jaarrapportage van FG leest, moet ook de wijze waarop de FG rapporteert aan de verantwoordelijke bestuursorganen nog formeel vastgesteld worden.

Momenteel **publiceren** we niet over de ontwikkelingen in onze gegevensbescherming naar burgers en inwoners. Dit is zeker het overwegen waard, bijvoorbeeld via de drie websites.

B. Kencijfers Privacy 2021-2022

Onderwerp	2021	2022
Uitgevoerde DPIA's	1	8
Aantal datalekken met meldingsplicht aan AP	6	11
Aantal datalekken zonder meldingsplicht aan AP	3	5
Aantal beveiligingsincidenten	1	2
Aantal verzoeken rechten van betrokkene (inzage, verwijdering, correctie)	5	5
Klachten over privacy in de organisatie	2	10
Aantal Fte's beschikbaar voor privacy	0,75	1

1. Toelichting DPIA's

In 2022 zijn er acht Data Protection Impact Assessments (DPIA's) uitgevoerd en landelijk vier DPIA's door organisaties zoals Vereniging van Nederlandse Gemeenten (VNG) die we (deels) kunnen hergebruiken.

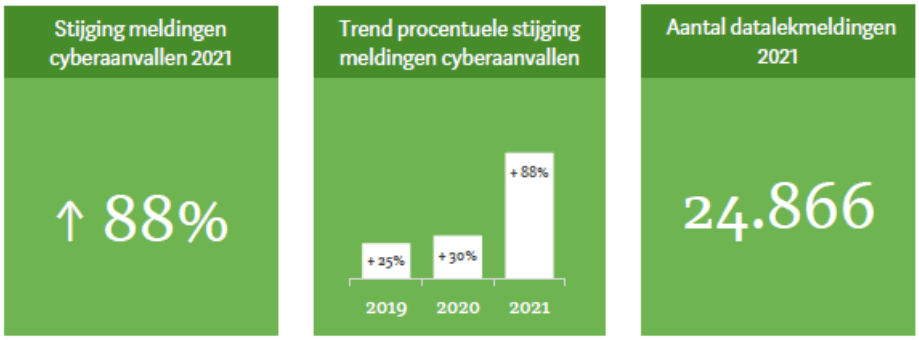
Belangrijk om te vermelden is dat de FG niet verantwoordelijk is voor de uitvoering van de DPIA's, die verantwoordelijkheid ligt bij de verwerkingsverantwoordelijke en proceseigenaar. De FG dient wel geraadpleegd te worden. Geconstateerd moet worden dat het uitvoeren van een DPIA nog niet goed is ingeregeld in de organisatie: de urgentie wordt niet gevoeld, de taken en verantwoordelijkheden zijn niet belegd en de kennis ontbreekt vaak.

Het dringende advies is om hier in 2023 echt werk van te maken en de meest risicovolle verwerkingen (of diensten, deelprocessen of systemen) te prioriteren en daarop DPIA's uit te voeren.

2. Toelichting Datalekken en beveiligingsincidenten

Landelijk beeld

Sinds 2016 moeten organisaties ernstige datalekken melden bij de Autoriteit Persoonsgegevens (AP). De AP publiceert elk jaar een totaaloverzicht van alle gemelde datalekken, de laatste is van 2021.



In 2021 ontving de AP 24.866 datalekmeldingen. Dat is een stijging van 4% ten opzichte van 2020 (23.976 datalekmeldingen). Het aantal meldingen van datalekken door hacking, malware of phishing (hierna: cyberaanvallen) is opnieuw fors gestegen. In 2021 waren er 88% meer van deze meldingen dan in 2020. Ook in 2020 en 2019 was er een stijging, respectievelijk van 30% en 25% ten opzichte van het voorgaande jaar. Het aantal cyberaanvallen omvat dit jaar 9% van het totaal aantal datalekmeldingen, vorig jaar was dit maar 5%.

Beeld WDW
In 2022 zijn er 2 beveiligingsincidenten in de vorm van een verloren/gestolen telefoon gemeld, hierbij zijn echter geen persoonsgegevens ingezien, gewijzigd of verloren gegaan. Het aantal datalekken bedroeg 16, hiervan zijn er 11 gemeld aan de AP en de betrokkenen.

De meest voorkomende datalekken zijn: foutief verstuurde e-mails en fysieke post. Oftewel e-mail of post gestuurd naar verkeerde ontvangers zoals collega's, externe behandelaars en verwerkers of raadsleden van de andere gemeente. De privacy-risico's waren gelukkig zeer beperkt. Ernstiger is dat in alle haast ook BSN-nummers van medewerkers per ongeluk terecht zijn gekomen bij een leverancier. Gelukkig betrof het een bekende, betrouwbare leverancier (verwerker) die de ontvangst direct meldde, de informatie heeft vernietigd en ons daarvan bericht heeft. En dat is precies zoals datalekken afgehandeld moeten worden: terstond melden en maatregelen treffen om de risico's te beperken.

3. Toelichting Rechten van betrokkenen

Betrokkenen hebben onder de AVG verschillende rechten om controle te houden over hun persoonsgegevens. In het jaar 2022 zijn 5 AVG-verzoeken binnengekomen bij de FG. Hiervan hadden 4 betrekking op het recht op inzage en een verzoek had betrekking op het recht op vergetelheid. Deze verzoeken zijn binnen de termijnen afgehandeld.

4. Toelichting Klachten van betrokkenen

Landelijk beeld
Sinds 25 mei 2018 kunnen mensen een klacht indienen bij de AP als zij het niet eens zijn met hoe een organisatie met hun persoonsgegevens omgaat. En zij er met de organisatie zelf niet uitkomen. De AP publiceert elk jaar een rapportage over deze klachten.

In 2020 heeft de AP heeft 25.590 klachten ontvangen. Een derde van de klachten had te maken met de privacy-rechten van burgers. Bijvoorbeeld klachten over organisaties die niet meewerkten als mensen inzage wilden in hun eigen gegevens of die gegevens wilden laten verwijderen. Daarnaast ging 15% van de klachten over het ongewenst doorgeven van persoonsgegevens aan andere organisaties.

Overigens zijn er 8% minder klachten ingediend dan in 2019. Deze daling komt echter vooral doordat het telefonisch spreekuur minder lang open was en er capaciteitsproblemen waren bij de AP. Er was gewoon minder gelegenheid om klachten in te dienen. De AP rondde 21.150 klachten af. Op 1 januari 2021 lagen er nog circa 9.800 klachten te wachten op behandeling.

De situatie in de WDW
In 2022 heeft de FG 10 klachten van betrokkenen ontvangen. Alle klachten betroffen persoonsgegevens die verwerkt worden in het kader van de gemeentelijke taken (en hadden dus geen betrekking op de verwerkingen in het kader van inkoop- of werkgeverschap door de WDW). De klachten zijn afgehandeld. Dit is wel aanzienlijk hoger als in 2021 (2 klachten). De oorzaak lijkt te zijn dat mensen de FG steeds beter en sneller weten te vinden, en dat mensen er meer en meer belang aan hechten om zelf goed zicht en controle te houden over de verwerking van hun persoonsgegevens.

5. Aantal Fte’s

In 2022 is het aantal fte’s voor privacy in de organisatie verhoogd van 0,75 fte naar 1 fte. Dit is een stap in de goede richting maar we zijn er nog niet. Zoals hierboven reeds vermeld, is het dringende advies om naast het formaliseren van de rol van de privacy-ambassadeurs en hen uren ter beschikking te stellen, ook een (of meer) privacy-adviseur aan te stellen (Privacy Officers). Dit mag worden verwacht van een organisatie van deze omvang en complexiteit.

C. Advies 2023

De constateringen en aanbevelingen in dit jaarverslag zijn erop gericht om een opgaande lijn te vinden en vast te houden. Daarvoor is op basis van de resultaten uit het borgingsproduct een prioritering gemaakt van verbeteracties. Hierbij is het uitgangspunt dat de organisatie ondanks beperkte capaciteit en middelen, dit toch aan zou kunnen én waar kunnen maken.

1. **Continue bewustwordingsproces**
   In 2022 is onderzocht hoe het bewustzijn rondom informatieveiligheid en privacy vergroot kan worden. Het advies is om:
   - Basiscursus informatieveiligheid en gegevensbescherming te verplichten voor alle medewerkers (voor nieuwe medewerkers reeds verplicht binnen drie maanden na indiensttreding)
   - Vakgerichte trainingen/workshops op teamniveau aan te bieden
   - Maandelijkse update, poll en privacy-vragen uit te zetten op intranet
   - Eens per halfjaar (juni en januari) een themabijeenkomst privacy en informatiebeveiliging te houden in de WDW- academie
   - Ludieke actie te starten om computerschermen goed te laten vergrendelen
   - Halfjaarlijks met het MT de stand van zaken betreft privacy te bespreken waarbij de cijfers en resultaten van het afgelopen maanden zullen worden gedeeld.

2. **DPIA-proces organisatie-breed inrichten en uitvoeren**
   Hoewel het aantal Data Protection Impact Assessments (DPIA's) in 2022 is toegenomen zijn we er nog niet. Het advies is om in 2023 echt ervaring op te gaan doen met DPIA's en te onderzoeken hoe het DPIA-proces goed ingeregeld kan worden.

3. **In kaart brengen van alle verwerkingen met grondslag toestemming**

4. **Uitwerken van de rechten van betrokkenen**
   In 2023 gaan we kijken hoe de rechten van betrokkenen zijn ingeregeld en hoe we dit proces, bijvoorbeeld een inzageverzoek, voor de burger kunnen versimpelen.

Notabene
Naast de AVG hebben onze boa's ook te maken met 'de andere grote privacywet: de Wet politiegegevens (Wpg). De Wpg regelt de verwerking van persoonsgegevens voor politietaken (politiegegevens), dat doen de boa's ook.

In het kader van de Wpg is in 2021 een externe audit uitgevoerd naar onze Wpg-compliancy. Dat rapport is eind 2022 beschikbaar gekomen. De hoofdconclusie is dat er ook voor de Wpg nog veel gedaan moet worden om werkelijk compliant te zijn. In 2023 worden hiervoor verschillende verbetermaatregelen getroffen en zal

een hercontrole plaatsvinden. Daarnaast zal de organisatie ook een interne audit naar Wpg-compliancy moeten uitvoeren.

Hoewel de AVG en de Wpg verschillende wetten zijn met eigen specifieke doelen en vereisten, delen ze hetzelfde uitgangspunt: ervoor zorgen dat organisaties de privacy van betrokkenen respecteren en te waarborgen dat persoonsgegevens op een veilige en verantwoorde manier worden verwerkt. Veel beheersmaatregelen die we moeten treffen voor de AVG, zijn ook verplicht voor de Wpg, bijvoorbeeld privacybeleid, datalekprocedure, autorisaties, bewaartermijnen, informatie-beveiliging en verantwoording, zij het dat de Wpg-eisen vaak net iets strenger zijn. Het verdient aanbeveling om de verbeteracties voor de AVG en Wpg goed op elkaar af te stemmen. Overwogen kan worden om hiervoor een apart programma in te richten.

Bijlage Definities

Autoriteit Persoonsgegevens (AP)	Onafhankelijke toezichthoudende autoriteit vanuit de overheid met onderzoeksbevoegdheden.[5] Wanneer een organisatie de opgelegde instructies niet naleeft, kan de AP corrigerende maatregelen te nemen zoals een waarschuwing geven, administratieve boete of last onder dwangsom opleggen.[6]
AVG	Algemene Verordening Gegevensbescherming
Betrokkene	Degenen van wie persoonsgegevens verwerkt worden.
Datalekken	Onder datalekken vallen onder de 'Privacywetgeving, inclusief de Algemene Verordening Gegevensbescherming. *"Een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan en er geen reservekopie is van die gegevens of als persoonsgegevens vatbaar zijn voor onrechtmatige verwerking."*
Data Protection Impact Assessment (DPIA) (GEB: Gegevensbeschermings-effectbeoordeling)	Een DPIA is een instrument om de privacy-risico's van een gegevensverwerking vooraf in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is verplicht als een gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor betrokkene(n).
Functionaris voor de Gegevensbescherming (FG)	De FG is degene die binnen de organisatie toezicht houdt op de toepassing en naleving van privacywetgeving (AVG en/of Wpg).
Privacy Officer (PO)	Privacy Officer (of PO genoemd) adviseert en ondersteunt bij privacyvraagstukken in de organisatie of in een specifiek domein. De PO heeft belangrijke rol bij de ontwikkeling en implementatie van beleid.

[5] Artikel 58 AVG.

[6] Artikel 58 tweede lid onder i AVG. Artikel 16 UAVG jo. Artikel 5:20 eerste lid AWB.

Three lines of defense model (3 LoD)	Uitgangspunt van het model is dat het lijnmanagement (de business) verantwoordelijk is voor haar eigen processen. Daarnaast moet er een functie zijn die de 1e lijn ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. Ook bepaalde beleidsvoorbereidende taken en het organiseren van integrale risk assessments zijn taken van de tweede lijn. De derde lijn controleert dan of het samenspel tussen de eerste en tweede lijn soepel functioneert en velt daarover een objectief, onafhankelijk oordeel met mogelijkheden tot verbetering. Dit is de afdeling interne audit, de FG en de CISO, die volledig los van alle andere organisatieonderdelen opereren.
Verwerkersovereenkomst	Wanneer een andere organisatie wordt ingeschakeld om voor de WDW/gemeente persoonsgegevens te verwerken moet een verwerkersovereenkomst worden afgesloten. Dit is alleen als de WDW/gemeente de organisatie de opdracht geeft om gegevens te verwerken waar de WDW/gemeente zelf verantwoordelijk voor is.
Verwerking	Alle handelingen met persoonsgegevens. *"Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens." (*artikel 4 tweede lid AVG)
Wpg	Wet politiegegevens